TOP SECRET **SUEDE**

NEVER TO BE SEEN BY UNAUTHORIZED PERSONS.

USSR

Ref. No: S/UQO-Z/
Issued : CB/OU/27.
Copy No: 20

RUSSIAN CRYPTOLOGY DURING WORLD WAR II

I N D E X

RUSSIAN CRYPTOLOGY DURING WORLD WAR II

I. Sources of Information.

A. Captured German Documents.

B. Home-Work of former German Cryptologic Experts.
1. Importance of these men.
2. Reliability of their evidence.

C. The Great Cryptanalytic Effort of the Germans against Russia.
1. The Continuity of effort.
2. The successes.

D. Interrogation of Japanese Cryptologic Personnel.
1. Difficulties in obtaining information.
2. Reliability of this evidence.

E. Evaluation of the Evidence.
1. Incomplete coverage.
2. Criteria for evaluation.
3. The period of validity.

II. Organization of Cryptology in the Red Worker and Peasant Army.

A. The Various Sections of the Red Army engaged in Cryptology.

B. The Authorized Strengths as of 1943.

C. The 8th Section of the General Staff in Moscow.
1. The subdivisions.
2. The functions of the cryptographic group.
3. The control of the Peoples Commissariat for Internal Affairs.
4. A strict selection of personnel.
5. The general reorganization of 1942.
6. The decentralization of production of cryptographic systems.
7. The reduction in training time for personnel.
8. Security measures.
9. Difficulties in subdividing the functions of the 8th Section of the General Staff.
10. The functions of the cryptanalytic group.
11. The functions of the technical group.
12. An opinion regarding the future.

III. Organization of Cryptology in the Peoples Commissariat for Internal Affairs.

A. The vastness of the apparatus and the consequent need for a communications system.

B. The centralization of production of cryptographic systems.

C. The decentralization of production of cryptographic systems for use of agents.

D. The high sense of responsibility of personnel handling cryptographic materials.

E. Lack of German knowledge regarding a Russian organization for cryptanalysis.

IV. Organization of Cryptology in Other Agencies.

A. The External Communications.

B. The Peoples Commissariat for Foreign Affairs.

C. The Peoples Commissariat for Foreign Trade.

D. The Communist-International.

V. The Basic Systems as found in Russian Cryptography.

A. Substitution Systems.
1. 2-figure codes.
2. Variable 1 and 2-figure codes.
3. 2-figure-letter codes.
4. 3-figure codes.
   a. The VAK-38.
   b. Other Books.
5. 4-figure codes.
   a. The OKK Books.
   b. The SUV Tables.
   c. Other Books.
6. 5-figure codes.
   a. The Chiffrecodes.
   b. Other Books.
7. The methods of re-encipherment.
   a. Methods which require a second step.
   b. Conversion tables.
   c. Additive sequences.
   d. Transpositions.
8. Indicator and Discriminant Groups.
9. Machine Methods.
   a. The Teletype.
   b. The K-37.

B. Transposition Systems.

C. Some Notes on Cryptographic Procedure.

VI. The Areas and Dates of Use of the Basic Systems.

A. In the Red Worker and Peasant Army.

B. In the Peoples Commissariat for Internal Affairs.

APPENDIX A.

A listing by DF numbers and title of all the documents covered in the preparation of this paper.

RUSSIAN CRYPTOLOGY DURING WORLD WAR II

I. SOURCES OF INFORMATION

A. Captured German Documents

The information presented in this paper is based solely on a study of relevant documents issued by the Armed Forces Security Agency (AFSA-14) in their TICOM Document Folder (DF) Series. The great majority of these documents are translations from the German of material pertaining to signals communications which the Target Intelligence Committee (TICOM) was able to salvage as cryptologic targets in German and German occupied territories on the continent of Europe were overrun by the advancing Western Armies in 1945. In addition to the discoveries of important Axis cryptologic caches, the interrogations of Axis cryptologic experts and the treatises written by some of them in the postwar era concerning their wartime activities have added to the amount of valuable documentary material.

B. Home-Work of Former German Cryptologic Experts

1. Importance of These Men

Of the treatises written in the postwar era, those written by the following cryptologic experts were found to be the most useful sources of information on Russian Cryptology:

Alex Dettmann, the former chief of the Russian Section of the Signal Intelligence Agency of the German Army High Command (OKH/Gd NA).

Kurt Friederichsohn, a linguist and cryptanalyst with the German Army Signal Intelligence Regiment (KONA 6).

Adolf Paschke, the last head of the German Foreign Office Cryptanalytic Section (Pers ZS).

Wilhelm Fenner, the former chief of cryptanalysis of the Signal Intelligence Agency of the Supreme Command German Armed Forces (OKW/Chi).

Wilhelm Flicke, formerly chief evaluator and the officially designated historian of the Signal Intelligence Agency of the Supreme Command German Armed Forces (OKW/Chi).

These men were key figures in the various German Signal Intelligence Agencies and there is no question but that they can speak with authority on the subject.

2. Reliability of Their Evidence

A general agreement regarding the details of many Russian systems is evident in these treatises. Only in a few instances may discrepancies be found. The information on the whole seems to be authentic and there is little reason to question the sincerity of these men. While these sources of information are often not as

extensive and detailed as one might wish, it must be remembered that these German nationals prepared their home-work from memory without benefit of extensive files which had long since been lost or destroyed. Of course in many instances, the descriptions are substantiated by captured documents which were obviously written before the German capitulation.

C. The Great Cryptanalytic Effort of the Germans Against Russia

1. The Continuity of Effort

That the German cryptanalytic effort against Russian military communications was very great is quite clear from even a cursory examination of these sources. And their undoubted successes in this field was due, according to Alex Dettmann, primarily to the fact that systematic observation of Russian military and political radio traffic and the cryptanalysis of it was begun early. While Dettmann certainly was not there at the beginning of the organization of German cryptology, there is available one source, namely Wilhelm Fenner, who was there, and is, therefore, in a position to give a detailed history of the skeleton forerunner of OKW/Chi and its connections with the other branches of the German Intelligence Service. When Germany collapsed in the fall of 1918 the Office of the Chief of the Signal Service was dissolved and of course all cryptologic work was supposed to be discontinued. However, Fenner states that he and one other man, Peter Novopaschenny, a former Imperial Russian Naval Captain, supposedly a director of the Czarist Russian cryptanalytic service against the German Baltic Fleet during the first World War, began in the autumn of 1921 the cryptanalysis of the telegrams to and from the Russian Military Attaché in Berlin. Thus did the Germans begin the rebuilding of their Cryptologic Agencies and such was the success that "Chi" itself (there were five other major German cryptologic agencies) in 1945 boasted that it had an invisible seat in the cabinets of more than 30 foreign governments, monitored currently some 300 cryptographic systems and read about 175 in 28 different languages.

The development of Russian cryptography shows how important it is to start decryptment of the cryptograms of a country whenever possible at a point where the cryptography of the country in question is still primitive. It is then necessary under all circumstances to continue observations of the traffic without breaks even for a brief period since otherwise ones own signal intelligence finds it difficult or even impossible to keep step with developments. The Germans did preserve such a continuity of effort against the Russians and as a matter of fact their continuity in this case was not even broken by the events of 1918, since Adolf Paschke says he was summoned in 1919 to the German Foreign Office as an expert in cryptology having had experience in cryptanalytic work with the Signal Service during the war 1914 - 18, and that during the years 1919 - 20 he did work through all the cryptographic material of the Czarist Foreign Ministry which had been preserved and made available to him.

2. The Successes

Mention of the following German cryptanalytic successes against the Russians during World War II is made in Volume I of the TICOM history produced at AFSA entitled "European Axis Signal Intelligence in World War II as revealed by "TICOM" Investigations

and by Other Prisoner of War Interrogations and Captured Material, Principally German":

a. The Signal Intelligence Agency of the Army High Command (OKH/Gd NA) established Russian army order of battle and location of strategic reserves from early in the war through 1943. This was accomplished through traffic analysis and cryptanalysis of Russian 2, 3, 4 and 5 figure codes (both Army and Peoples Commissariat).

b. The Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350) by cryptanalysis of Russian Air Force ground-to-ground 2-figure, 3-figure, and 4-figure administrative and operational codes, and some 5-figure codes, provided a complete order of battle for the Russian Air Forces from 1937 until the end of the war. From partial decipherment of air-ground traffic, from plane-to-ground radio-telephone monitoring, and from radio-direction finding of bombers when airborne, this agency was able to give accurate warnings of all Russian long-range strategic bombing raids. Also from cryptanalysis of each Russian Air Army's 2-figure, 3-figure, and 4-figure traffic, from traffic analysis, from plane-to-plane radio-telephone monitoring, and from radio direction-finding of planes in flight, it was able to warn German ground forces and fighter squadrons of impending operations by Russian fighters and fighter bombers.

D. Interrogation of Japanese Cryptologic Personnel

1. Difficulties in Obtaining Information

In addition to the German sources of information there must be mentioned the fact that due to the eminent success of TICOM operations in the European Theatre of Operations, similar measures were taken for the exploitation of Japanese cryptologic targets. For various reasons, chief of which were the diplomatic nature of the surrender and the delayed occupation, TICOM activities in the Pacific Theatre did not meet with a similar success. The Japanese authorities in the field of Signal Intelligence, having recovered from the initial numbing impact of the surrender, were able to destroy much which might have been of importance and to instruct their subordinates regarding the extent to which they should cooperate with the investigating parties and the amount of information to be revealed. It was found, however, that the Japanese did achieve some degree of success in the cryptanalysis of Russian systems.

2. Reliability of this Evidence

A study of the translations of the TICOM interrogations of the Japanese so far issued in the DF series gives the impression that this source of information is rather vague and clouded as regards the treatment of Russian cryptology. There is certainly not the sincerity and straightforwardness of thought that is evident in the German material on this subject. This source seems to add little to the information on Russian cryptology obtained from the German material, and this is to be perhaps more or less expected, since it is estimated that the six main cryptologic organizations possessed by Germany during World War II had a total strength including field units and overhead of approximately 30,000 persons.

E. Evaluation of the Evidence

1. Incomplete Coverage

While it is evident from the above outline of the sources of information that much may be learned regarding Russian Cryptology, especially so from captured German documents and interrogations of former German signal intelligence experts, it must be emphasized that since all the TICOM material in repository at Government Communications Headquarters (GCHQ) and Armed Forces Security Agency (AFSA) has not yet been processed (1951) and since the total of processed material from AFSA on file at CB represents only a small percentage of that issued, it is quite possible that the results of this survey might be augmented and some details revised if a more complete examination were possible. Only translations of TICOM documents issued in the DF series have been examined; other TICOM documents, such as those issued in the D (Document) series and I (Interrogation) series may throw further light on the subject.

2. Criteria for evaluation

Details of the organization of the Russian Communications Security Organization and descriptions of the cryptographic systems used together with the areas, authorities, and dates of issue and recall are here summarized from the documentary material that is available. A complete listing by DF number and title of all the documents studied will be found in Appendix A.

The following criteria for evaluation will be followed in this paper:

a. Captured documents are considered the more reliable.

b. The German interpretation takes preference over the Japanese.

c. In the case of dependence on reports written after capitulation the version of Alex Dettmann is taken above all others inasmuch as he was not only the chief of a department specializing in decryption of Russian systems but also had a continuity of successful effort in this field for over ten years.

3. The Period of Validity

The period of validity for the statements made in this paper will cover roughly the period 1935 to 1945, unless otherwise specifically stated. It was during this period that the Germans who are our main sources of information, made their great cryptanalytic effort and achieved many successes in reading the ciphered communications of the Russians. It should be noted that we have here retained the Russian nomenclature as interpreted by the Germans during that period. Thus, for example, the term NKVD (Peoples Commissariat for Internal Affairs) is no longer current, the equivalent organization now being called MVD (Ministry of Internal Affairs).

II. ORGANIZATION OF CRYPTOLOGY IN THE RED WORKER AND PEASANT ARMY

A. The Various Sections of the Red Army Engaged in Cryptology

The highest agency for cryptology in the Army and Air Force of the U.S.S.R., both for Communications Security and Communications Intelligence as well as for the related technical fields, is the 8th Section of the General Staff of the RKKA (Red Worker and Peasant Army) in Moscow. Directly subordinated to it are all 8th Sections of the front staffs, armies, and corps, and all 6th sections of divisions and brigades as well as the SHO (cipher sections) of the lower echolons. After July 1942 the designations of the cryptographic sections of armies and corps seem to have been changed to 6th Sections.

B. The Authorized Strengths as of 1943

From numerous P/W interrogations of Russian cryptographic officers, the Germans reported the authorized strengths for these cryptographic sections in 1943 as follows:

General Staff 8th Section Cryptographic Group	400 men	
Front Staff 8th Section Cryptographic Section	65 men	Chief has rank of Colonel.
Army Staff 6th Section	20 to 22 men	Chief has rank of Lt. Colonel.
Corps Staff 6th Section	10 men	Chief has rank of Major.
Division Staff 6th Section	5 to 6 men	Chief has rank of Captain.

Brigades and other units subordinate to a division down to battalion have only a cryptographic officer assigned to the responsible staff as "Assistant to the Chief of Staff for Special Communications".

C. The 8th Section of the General Staff in Moscow

1. The subdivisions

The 8th Section of the General Staff of the RKKA in Moscow is said to be subdivided according to its duties into three groups, each of which assumes a number of functions:

Group I. Cryptographic

1. Administration and personnel.
2. Development and current improvement of cryptographic systems.
3. Introduction and distribution of Cryptographic materials.
4. Registration of all encrypted messages in operational and tactical systems.

Group II. Cryptanalytic

1. Cryptanalysis of foreign cryptographic systems.
2. Commitment and organization of radio reconnaisance.
3. Evaluation.
4. Archives for captured documents.

Group III. Technical

1. Development of cipher machines and testing of proposals in this field.
2. Development of mechanical aids, possibly cryptanalytic machines; may also be concerned with the generation of infinite digit sequences to be distributed in the form of "Bloknots" (one time additive pads).

2. The Functions of the Cryptographic Group

Group I or the Cryptographic Group is for all practical purposes, the administration of the 8th Section. In close contact with the NKVD (Peoples Commissariat for Internal Affairs) it is responsible for seledtion and maintenance of cryptographic personnel. It sets up training courses and distributes the trained men according to needs.

The preparation and distribution of new cryptographic materials as well as the withdrawl of those to be replaced was exclusively the duty of Group I of the 8th Section of the General Staff of RKKA in Moscow till March 1942. In this way a unified direction and control was possible and the issue of only a few general systems had the advantage that these were well mastered by the cryptographic personnel and that errors in encryptment could generally be avoided. It is obvious that this type of unified direction was also of great advantage for German cryptanalysis because a concentration of homogeneous traffic made possible a break into Russian systems and the relatively long period of use of the single system made possible the expansion of these breaks by the Germans.

3. The Control of the Peoples Commissariat for Internal Affairs

That the NKVD exercised an overall control in the compilation and distribution of cryptographic materials and a surveillance of cryptographic personnel in 1939 is definitely proven from a Russian document, "Regulations for Staff Cryptographic Service in the Red Army" (DF 95). The document captured by TICOM is the German translation of the Russian regulations published by the 8th Section of the General Staff of the Red Army Moscow, 1939. The following excerpts from this document should be sufficient:

Para 9. "The entire work of the staff cryptographic units in the Red Army is directed by the chief of the war commissar of the Red Army through the 8th Section of the General Staff. In their technical (special) activities the staff cryptographic units are guided by instructions of the 7th Section of the Main Administration of State Security of the Peoples Commissariat for Internal Affairs of the Soviet Union (GUGB NKVD SSR)."

Para 28. "Ciphers, their component parts, the instructions for their use, are compiled, put into force, and declared invalid, in the Red Army only by the General Staff of the Red Army through the 8th Section of the General Staff. Every cipher must be worked out in agreement with the 7th

Section of the Main Administration of State Security of the Peoples Commissariat for Internal Affairs for the Soviet Union."

4. A Strict Selection of Personnel

In the selection of communications personnel, in particular those dealing with cryptographic material, extraordinary strict standards were applied until the beginning of 1942. All those engaged in the 8th Section or its subordinate organs, even down to the last "SHO" co-worker in the smallest unit had to be old party members and absolutely reliable in their political attitude. In the final analysis, therefore, the selection of this personnel was completely under the control of the NKVD.

Likewise, the two special schools for cryptographic personnel in Moscow and in Tambov were conducted by the NKVD. Before the war and down to early 1942 the period of training at these schools was six months. Besides training in the handling of the most varied cryptographic systems, there was taught in condensed form the history of cryptography and the field of cryptanalysis was touched upon briefly. However, it is certain that no decryption of any type of foreign cryptograms was taught or practised at these schools and that the brief glimpse of cryptanalysis was only intended to demonstrate to the pupils that such a thing existed and to train and inspire them to precise, responsible use of cryptographic material. On completion of this training course for the perfection of officers of the staff cryptographic service (KUKS) an examination was required.

5. The General Reorganization of 1942

The RKKA as a whole underwent a speedy reorganization during the first winter (1941-42) of the war with Germany. All measures which up till then had given the war on the Russian side a Communist-International character were very cleverly changed and the war was declared a campaign for the freeing of the Fatherland -- the Patriotic War with the German Fascist Aggressors. The NKVD has a system of political guidance and leadership reaching from the General Staff of the RKKA down to company platoons. In addition to the official representatives of the NKVD there are secret agents from the ranks of the Red Army working under them, whose task it is to recognize and report in their initial stages any movements hostile to the Soviets. Arrest and punishment lie in the hands of courts martial conducted by the NKVD. In the reorganization the political commissars who up till then had to countersign every order of the commanders and exercised an often fateful influence on the morale of the troops, disappeared officially. Nevertheless an invisible political surveillance by the NKVD continued, unreliable commanders were transferred and thus disappeared more or less without attracting attention.

6. The Decentralization of Production of Cryptographic Systems

The rapid German advance during the summer and autumn of 1941 with great encirclement battles and unforseen flank and pincer movements inevitably resulted in the German capture of numerous Soviet cryptographic documents of the Army and Air Force. Since when they were used universally the capture of a single copy was sufficient to compromise the system of the entire front, it was obvious that the Soviet Supreme Command had to make a change as quickly as possible. This basic change in the organization of the cryptographic service in a period which was exceedingly

critical for the USSR was put through in the notably brief period of three months, using threats of the severest penalties for any delays or contraventions, and by the expiration of the month of March 1942 was everywhere completed. In contrast to the centralization of peacetime, the production and distribution of cryptographic material was now decentralized. Group I of the 8th Section of the General Staff of RKKA in Moscow remained responsible only for the issue, recall and replacement of the operational 5-figure code (Chiffre) and had to provide current means of reencipherment (additive sequence) for this cryptographic system. All radio messages in this most important Russian system were sent in the original, after they had fulfilled their immediate purpose, to Group I of the 8th Section and were here sorted and filed from the point of view of military history. They were intended to form the basis for a subsequent general staff study.

With the decentralization, all cryptographic systems used at the front - called since then SUV, (camouflaged communications of the Command) - were worked out by the Signal officers of the immediately superior units, were issued at their discretion, and were likewise replaced when there was danger of compromise. The systems thus originated were distributed to the subordinate units and to the neighbouring organization - from left to right. For the setting up and working out of SUV systems by the individual Signal Chiefs a scheme was worked out by the 8th Section of the General Staff in Moscow which outlined in a general way the size and type of such cryptographic systems but contained no directive regarding the choice of the reencipherment.

According to Alex Dettmann it is solely due to this change in the organization of the cryptographic service that the readability of Russian army messages became much less and that the capture by the Germans of such cryptographic systems no longer represented a danger to the entire front. The multiplicity of these systems, the relatively slight amount of traffic on the individual net and the short period of use made analysis extremely difficult and often made the work on very small groups of messages an impossibility. If in spite of this it was possible for the Germans right down to the final days of the war to provide their High Command with important information, often when their own communications system was having great trouble, that was due exclusively to the fact that the former German Army had plenty of trained and experienced cryptanalytic personnel.

7. The Reduction in Training Time for Personnel

The heavy losses suffered by the Russians in the summer and autumn of 1941 was also felt among their cryptographic personnel. It became necessary to change the requirements regarding selection and to reduce the period of training at the special schools for cryptographic personnel. The Russian with his ingrained tendency to allow only the smallest possible number of people any insight into secret matters had not been able to make provision for the loss of trained people and provide trained replacements at once; he was therefore obliged to give up an all too strict and thorough selection of cryptographic personnel. Since 1943 non-members of the communist party could be employed as cryptographers, if they were otherwise dependable. The period of training which was first reduced to three months was again reduced and since 1943 was only one month. As a result of the heavy losses, the personnel strength of all the 8th and 6th Sections had to be sharply reduced and the heavy losses of officers in particular resulted in the employment of

civilian officials as directors of the 6th Sections with brigades and divisions.

As a consequence of the cuts in personnel and training time which occurred in various parts of the Signal Service in 1942, the performance and reliability of radio operators and cryptographic clerks suffered. More errors occurred in encrypted messages and frequent requests for repetitions or for changes of key were noticed by the Germans on many Russian links. This fact is doubtless one of the reasons for the rapid extension of Baudot lines in internal communications since in this way it was possible to spare communications personnel in the interior for service at the front. Whether in addition to Baudot, cipher teleprinters, speech scrambling machines, or pure cipher machines were also put into use on internal circuits is not quite certain. However it seems definite that traffic in machine systems had not appeared on military circuits up to May 1945. Dettmann is of the opinion that the Russian prefers manual methods of encryptment, all the more so since he has found in the use of the one-time additive the ideal method of re-encipherment.

8. Security Measures

Interesting and illuminating as regards the importance of secrecy in the Russian Cryptographic Service is the fact that the sections working with ciphers at the individual staff could only be entered by the Commander, his deputy, and the highest political functionary (NKVD), and that, aside from the Section Chief of the moment, only these had the right to check the work of the individual cipher clerks. The cipher clerk, however, was only permitted to take orders from his immediate superior, i.e. the chief of the section concerned. Since the chief of the cipher section, at least in the first year of the war was an old party member and thus very often closer to the political functionary of the unit than the commander, there were often disagreeable conflicts which might ultimately lead to an absolute split between the political and military leadership. In any case down to the middle of 1942 it was practically impossible for the Commander to send a report by radio without the knowledge and counter signature of the Commissar whether to a superior office or only to subordinate formations. This untenable situation came to an end with the basic changes in the course of 1942. The competences of the political leadership were clipped in harmony with the proclamation of the war as a Fatherland crusade and the commanders now obtained the right to make their decisions themselves. Practically, however, everything remained the same, since the Commissar still had the right to read all messages and could, if he chose, use these as proof against the military leadership.

That the NKVD was ever present in the Russian Cryptographic Service is seen from the following references to security to be found in the above mentioned manual, "Regulations for Staff Cryptographic Service in the Red Army".

Para 45. "The destruction of cryptographic issues which have been declared invalid is carried out by the cryptographic units of districts and army staffs on the basis of instructions from the 8th Section of the General Staff of the Red Army. Destruction is in accord with instructions given in Section 114 of these regulations but only in the presence of a representative of the 7th Section of the GUGB NKVD SSSR (7th Section of the UNKVD)."

Para 123. "If any breach of these regulations or any absence of basic documents is disclosed, the chief of the staff cryptographic unit inspected is obligated to take steps immediately to eliminate such breaches and also to search for lost documents. At the same time a report is to be made to the cryptographic unit of the next higher staff, to the 8th Section of the General Staff of the Red Army and to the local organ of the NKVD."

In connection with security measures it is interesting to note that as early as 1939 the Russians were aware of the fact that radio is not the most secure means of communication and that the use of land lines whenever possible was ordered. Quoting again from the above manual:

Para 27. "Ciphers are intended exclusively for the transmission of strictly secret and secret messages of an urgent nature. The transmission of enciphered messages by radio is only permissible in exceptional cases, i.e. in default of wire connections, whereby the special instructions of the General Staff of the Red Army are to be followed."

9. Difficulties in Subdividing the Functions of the 8th Section of the General Staff

The organization and functions of the Cryptographic Group (Group I) of the 8th Section of the General Staff of the RKKA in Moscow have been covered in some detail and the overall control of the NKVD, visible or otherwise, in these matters seems beyond question. While there is general agreement as regards the functions of Group I there seems to be some doubt concerning those of Group II (Cryptanalytic) and Group III (Technical). Alex Dettmann, the former chief of the Russian Section of OKH/Gd NA points out that the structure of the 8th Section of the General Staff in Moscow and its functions could not be the subject of enciphered communications and that knowledge regarding it must be secured from other sources. Dettmann, maternally of Russian stock and an expert in the language, claims to have personally conducted many of the interrogations of prisoners and deserters suspected of having had official connection with these matters. He is quite definite in the statement that the 8th Section of the General Staff had a group engaged in the cryptanalysis of enciphered enemy reports. (DF 112 and 196). This was also undoubtedly the official opinion in the Signal Intelligence Agency of the German Army High Command as expressed in a captured document from that agency dated to 1943. (AFSA-14 Serial 5/49). However, one discordant note is found in the report of an interrogation conducted by Sergius Samsonow (the deputy of Dettmann and also a key figure in German Army Signal Intelligence) in 1944. (DF 89). The Russian prisoner who was evidently especially interrogated by Samsonow, was a former chief instructor in the Cryptographic School at Tambov. In the translation of this German report there is found the following:

"Cryptanalysis and cryptographic security study is not carried on within the Red Army. Sections concerned with such duties are assigned neither to the General Staff nor to the subordinate staffs. The interception of enemy radio traffic is controlled without exception by the 5th Section of the NKVD in Moscow. This 5th Section of the NKVD is the only organization that is concerned with cryptanalysis and security studies. Pavlov

knows nothing further on this organization or the nature and results of its operations. The introduction of a new code or a new system by the 8th Section of the General Staff is carried out in all cases only with the approval of the 5th Section of the NKVD, where the "security" of the proposed system is tested. There has often been discussion that the control of the 8th Section of the General Staff lies in the hands of the chief of the 5th Section of the NKVD. Within the army there is actually only work with direction finding and the interpretation of enemy call signs."

Note that the control exercised by the NKVD over the introduction of new cryptographic systems was reported in the excerpts from "Regulations for Staff Cryptographic Service in the Red Army" (1939) as being not in the 5th but in the 7th Section of the Main Administration of State Security of the Peoples Commissariat for Internal Affairs of the Soviet Union (GUGB NKVD SSSR).

Furthermore it may be safely assumed that the conclusions expressed in the translation of the captured document (AFSA-14 Serial 5/49) were the result of the sifting of many such interrogations by the Germans and that the 8th Section of the General Staff in Moscow was therefore engaged in the cryptanalysis of enemy radio traffic with an overall control being exercised by the NKVD.

But in view of what has already been pointed out regarding the Russian concept of security, it seems hardly likely that these prisoners would be able to give many details regarding the technical work of the 8th Section of the General Staff and certainly no details of Russian successes in cryptanalysis, since personnel possessing such technical knowledge would not have been found by the Germans in a combat area. Even in the field of cryptography, the Germans found that again and again they themselves were often better informed regarding Russian systems than the cryptographic officer being questioned since he knew only his own system, the one he was working with at the moment and could tell at most the systems with which he had worked previously.

10. The Functions of the Cryptanalytic Group

The cryptanalytic group or Group II of the 8th Section of the General Staff in Moscow is said to deal with the cryptanalysis of foreign cryptographic systems, the organization for traffic analysis and interception of such systems, and the evaluation of the products of traffic analysis and cryptanalysis. Dettmann writes that according to the statements of prisoners, deserters and agents, primary importance was given traffic analysis, direction finding and observation of operations while cryptanalysis was able to show only scant results in spite of extensive employment of personnel. However, considering the Russian mentality, their aptness and talent for mathematical matters and secret affairs, it would be very strange indeed, if the large staff of scientific employees, including linguists and mathematicians, said to have been active in cryptanalytic work in the 8th Section of the General Staff in Moscow did not achieve at least some success in this field.

While very little is known regarding the successes or lack of successes of the cryptanalytic work in the 8th Section of the General Staff of the RKKA in Moscow, it is clear that Russian traffic analysis was able during the war to achieve

very considerable successes to the sorrow of the German command by intensive use of men and equipment and uninterrupted observation of various German circuits. Thus for instance the Russians monitored with great persistence the arrival and departure of German planes at all sorts of airfields. An antiquated system of call signs on the German part often gave them a chance to determine the number of planes and their type and to recognize what they were doing. Far more unpleasant for the German front in the East, which was often very thinly held in insufficient depth, was the fact that the Russians by studying indicator groups and by direction finding recognized the joints in the German front and concentrated their attacks on these points which, as everyone knows, are likely to be the weakest. This is the considered opinion of Alex Dettmann.

Especially interesting from the point of view of Russian techniques in traffic analysis is DF 143, "Manual for the Analysis and Utilization of Radio Intelligence Material." It is a draft translation of a Russian manual published by the Intelligence Department of the General Staff of the Red Army, Moscow 1944. Chapter I deals in detail with the information to be obtained from radio intelligence, its importance and method of utilization, Chapter II covers the basic types of radio nets, Chapter III is on direction finding service and analysis of bearings, and Chapter IV gives methods of analyzing and utilizing radio intelligence data. This Russian manual was designed for the tactical level and careful perusal of it leaves the impression that the Russians possess a highly sophisticated concept of communications intelligence. And if this be so then it is probable that they are equally proficient in the related field of cryptanalysis.

This assumption is further confirmed when it is realized that from the degree of security evidenced by the cryptograms of a given country can be deduced with absolute certainty the existence and extent of a cryptanalytic unit and its direct influence on the cryptographic systems of the country.

For example, when simple codes and superencipherments are used side by side, then in times of increased activity experience shows again and again that if adequate controls are lacking code clerks pressed for time encrypt messages with secret content in simple code in order to save the time required for encipherment.

Proof that the cipher personnel has not been trained by experts of the cryptanalytic service and is not constantly supervised by such experts is found also in less pronounced cases, such as, carelessness in giving preference to certain indicator groups or the often unconscious preference for certain rows and similar phenomena of which the code clerk is unconsciously guilty.

If, now, such breaches of security are not to be observed in the encrypted traffic of the USSR or are limited to rare exceptional cases, it is possible to deduce from this fact that the Russian cipher personnel is either far superior to that of other countries in training and awareness of its obligations or that the handling of all systems by the cipher personnel is subject to such strict and regular control that such errors or habits are either avoided entirely or are discovered at once and stopped. Since the former possibility is not very likely, only the second explanation remains.

Furthermore it must be assumed that this control - because of its effectiveness - is in the hands of cryptologists because only they have the necessary experience to recognize at once all mistakes which are likely to compromise a system.

11. The Functions of the Technical Group

Dettmann reports that before the reorganization of the RKKA in 1942, the task of working out new cryptographic material was divided between Group I (Cryptographic) and Group III (Technical). While the technical group undertook the purely theoretical development according to cryptologic principles, the cryptographic group checked these with respect to suitability and convenience. That is, the cryptographic group had the final (RKKA) word as regards introduction and distribution of cryptographic materials. The generation of infinite digit sequences to be distributed in the form of one time additive pads was also probably done by the technical group. The compilation of systems of call signs and the allocation of wave lengths is said to have likewise been done by this group. The technical group seems therefore to have been concerned with the actual production of cryptographic materials. Beyond that it is supposed to have been occupied with the development of cipher machines, possibly also cryptanalytic machinery, and the checking of inventions and proposals received from outside sources. After the shift in 1942, it is said that the technical group devoted its principal attention to the development of Baudot equipment and circuits.

12. An Opinion Regarding the Future

It has been pointed out how the development and issue of cryptographic material in the Red Army was centralized up to March 1942 in the 8th Section of the General Staff in Moscow and how the course of the war with Germany brought about the decentralization which was in effect until the end of that war in 1945. As regards the future, Alex Dettmann ventures the opinion that the 8th Section of the General Staff in Moscow may, now that the war is over, return to the former centralization of the development and issue of cryptographic material. There are two very good reasons for the Russians to make such a change. In the first place, the administration and control of the elaborate apparatus can be handled much more easily in this way and, in the second place the sole reason for the change in 1942 - the possibility of capture by the enemy of secret documents - no longer holds.

III. ORGANIZATION OF CRYPTOLOGY IN THE PEOPLES COMMISSARIAT FOR INTERNAL AFFAIRS

A. The Vastness of the Apparatus and the Consequent Need for a Communications System

Before presenting the few details that are known concerning the organization of Cryptology in the NKVD (Peoples Commissariat for Internal Affairs) it might be well to stress the importance of this organization in the political, military, and economic life of the Soviet Union.

The basic task of the NKVD was to assure the continuance of the political structure of the USSR. To carry out the necessary measures the NKVD had at its disposal various types of troops of its own - NKVD troops - which were assigned and employed according to need by the Central Office in Moscow (GUP NKVD, Central Administration of NKVD Troops).

From an evaluation of the results of traffic analysis and cryptanalysis on Russian traffic the Germans were able to establish the following catagories of NKVD troops:

Troops of the Interior - The "Political Section NKVD" has an extensive network of agents to note any trend hostile to the Soviets. The actual combatting of any such movements is by contingents of these "Troops of the Interior." When there was an occupation of foreign territory during the war, the number of political sections increased materially with consequently a very great increase in the number of contingents of "Troops of the Interior" NKVD.

Escort Troops - The sending away of politically unreliable elements, surveillance, and control of concentration camps as well as the setting up of penal camps and penal battalions fall in the province of the "Escort Troops" NKVD.

Frontier Troops - Because of the special political structure of the USSR, it was necessary to provide for sealing the country hermetically from the outside world. This is the function of the "Frontier Troops" NKVD. Corresponding to their task, these troops have aircraft available and along the water boundaries, appropriate watercraft. Before the war these troops were deployed along the actual frontiers but with the outbreak of hostilities regiments of "Frontier Troops" NKVD were employed some 30 to 60 kilometers behind the combat units of RKKA (Red Worker and Peasant Army) to form an unbroken, very mobile, and deeply deployed security zone. NKVD forward staffs controlled the employment of these regiments; these staffs were located in the immediate vicinity of the forward staffs of the Army but received their orders from NKVD headquarters in Moscow. The task of this security zone was to prevent desertion and infiltration of enemy agents by sealing the sector of the front from the rear area; by mopping up pockets, and clearing areas near the front of cut-off enemy troops and bands; by removal or resettlement of the populace for political reasons; by return of population for repair or new construction of roads, defense installations, air fields, and plants of value to the military economy; by guarding supply; and by collecting and transporting prisoners to the rear.

Railway Troops - The entire economy of the Soviet Union, in particular the military economy and transportation system are under very sharp control and thus under the influence of the NKVD. Whereas before the war this control could be exercised through the local organs of the NKVD, after the outbreak of hostilities it became necessary to take over also the protection

of the railroads along with their control and for this purpose especially trained troop contingents, "Railway Troops" NKVD were formed. They guarded transports, depots, bridges, junction points, and important as well as threatened stretches of railway track.

Operative Troops - In various phases of the war the need appeared for very daring and reliable units at danger points in the line or at points of concentration. Such elite troops were formed by the NKVD and assigned to divisions of the RKKA armies as "Operative Troops" NKVD.

In addition to the major tasks already outlined the NKVD was charged with the carrying out of the following supplemental tasks: (1) The political training of the RKKA by means of political units, political commissars, etc. (2) The training of a number of military specialists, such as sharpshooter units; selection and training of all replacements for medium and high-grade officers in the RKKA, and all technical signal personnel including those engaged in cryptographic work. (3) The conduct of training schools for dogs and carrier pigeons. (4) The combatting of espionage, sabotage and the activity of enemy agents. This work was done by the SMERSH (Death to Spies), an agency under the control of the NKGB (Peoples Commissariat for the Security of the State). (5) Direction of the activities of partisans and the training of agents for work behind the German front. (6) Mobilization and drafting of recruits for the RKKA. (7) Recruiting workers from among the people of occupied areas into labor battalions. (8) Integration of armies and units of foreign nationality into the framework of the RKKA.

With such a powerful organization having tentacles which reach into the furthermost crevices of the political, military and economic life of the Soviet Union, it is obvious that the NKVD must also have possessed a far-flung communications complex and cryptographic systems of its own.

B. The Centralization of the Productions of Cryptographic Systems

It is said that the Central Office for the cryptographic service of the NKVD organs was located with the GUP NKVD (Central Administration of NKVD troops) in Moscow. Organization and functions of this section in the field of cryptology are not known. In contrast to the cryptographic systems of the Army and Air Force, no cryptographic systems of the NKVD were ever captured by the Germans while they were still in use. At various points on the front 4-figure NKVD codes did fall into the hands of German troops, but either they were then no longer in use or they represented reserve systems which, due to their capture, were not put into use. Consequently there was never the urgent need which brought about the decentralization already noted in the case of RKKA cryptography but instead the NKVD Cryptographic Central Office in Moscow was able to retain the method of centralization for the production, issue and recall of cryptographic material throughout the entire war. For this reason the Section of GUP NKVD corresponding to the 8th Section of the General Staff of the RKKA in Moscow was not obliged to make any radical change in the further development of cryptographic systems but allowed them to remain substantially unchanged from the time the Germans began systematic observation down to the day of capitulation. Therefore in spite of the great number of different NKVD organs there was only a very limited number of NKVD cryptographic systems in use and it was also true that these were valid for a relatively long time, often more than two years. Consequently there was the chance

for the German cryptanalysts to do extensive work on great amounts of homogeneous material and to accomplish more with far less personnel against NKVD cryptographic systems than was the case with RKKA systems.

All internal radio circuits of the USSR were not only monitored and controlled by the NKVD but in many cases were directed by it and in all probability the GUP NKVD was also responsible in large measure for the issue of any cryptographic material which might be used for encipherment of such internal radio traffic. The Germans of necessity gave some attention to the interception and decryptment of this traffic. Among other things, special units were devoted to the reception of the Baudot traffic passed on many of these circuits by high-speed transmitters. It is reported that of the entire traffic monitored at great expense by the Germans, at best only 10% was useful for economic leaders while military-political matters constituted hardly 1%. From this traffic German evaluation results lay almost exclusively in the economic field.

C. The Decentralization of Production of Cryptographic Systems for use of Agents

The NKVD also had an important share in the preparation and issue of cryptographic materials for partisan organizations and for the agents and espionage service. In view of the initial multiplicity of partisan groups which operated independently and of the often very extensive employment of agents and spies in the enemy's rear, it was necessary to provide for current replacement of cryptographic systems, in which connection it was of primary importance that these should be convenient, simple to use, and yet secure. This responsibility could not be met by a single central unit, however large; therefore the individual partisan staffs, which for the most part were located in the immediate vicinity of army front staffs, were assigned the task of producing and distributing such cryptographic systems, although all of them were subject to the guidance and control of the NKVD. Although the systems used in partisan, scout, and agent traffic, from the simplest to the most difficult, included some which were neither theoretically or practically capable of solution, it can be stated with good reason that in many respects much latitude was afforded the individual imagination and discretion. A norm, similar to that in the SOV systems of the RKKA, did not exist. The structure and use of cryptographic means had to be adapted here to the momentary needs of agents who often worked alone.

D. The High Sense of Responsibility of Personnel Handling Cryptographic Material

Considering the vastness of the NKVD apparatus and its consequent use of a complex communications system, one unique characteristic was noted by the Germans during the war. This is the high degree of training and the sense of responsibility of NKVD personnel which prevented any cryptographic systems of the NKVD which were still in use from falling into the hands of the Germans during the entire period of the war. This is indeed amazing since the Germans proved conclusively time and again throughout the course of the war that the complete destruction of all secret documents of a nation is a practical impossibility. According to the German account of their experiences in the Balkan Campaign, the Greek and Yugoslav Governments had obviously issued orders for the destruction of all secret documents, yet the amount of captured material was so enormous that it had to be shipped in barges up the Danube to Vienna and from there to Berlin in freight

cars and nearly two years elapsed before a systematic evaluation of these documents was finally concluded by the Central Evaluation Section in Berlin. But during the German advance into Russia, up to the seige of Stalingrad in 1942, the operational area of the Frontaufklarung (military intelligence in the operational area) comprised upwards of 3 million sq. kilometers of Russian soil and although many, many documents had been abandoned by the Russians in the battle and contrary to orders, over 3,000 comprising only the most important ones having then been registered at Walli III (the German center for tactical counterintelligence on the Eastern Front), still no live cryptographic material of the NKVD was found at this time or even during the entire period of the war. In this connection it might be mentioned that our own TICOM effort against the Germans which saw the first exploitation team dispatched in April 1945 was able to salvage approximately 4000 separate German documents with a weight of about 5 tons and this does not include materials captured in the heat of battle and passed to military intelligence for immediate processing.

E. Lack of German Knowledge Regarding a Russian Organization for Cryptanalysis

Not a thing is known about the possible activities of an agency of the NKVD in the field of cryptanalysis. The subject has already been touched on above in the discussion of a similar function being exercised by the 8th Section of the General Staff of the RKKA. The conclusion is that the NKVD is active, whether in absolute control or merely maintaining its customary surveillance in a more subtle way, it matters little.

IV. ORGANIZATION OF CRYPTOLOGY IN OTHER AGENCIES:

A. The External Communications

In the organization of cryptology in the Soviet agencies so far mentioned we have been concerned for the most part with strictly internal communications. When we come to an examination of the external communications of the USSR, at least three agencies are mentioned by the Germans as using cryptographic materials during this period. In the diplomatic field we have the Peoples Commissariat for Foreign Affairs, in the commercial field the Peoples Commissariat for Foreign Trade, and in the communist-international field the Comintern as it was called at that time.

B. The Peoples Commissariat for Foreign Affairs

No mention is found in these sources regarding the authority for the compilation, issue and recall of the cryptographic materials used by the Peoples Commissariat for Foreign Affairs. But in view of what has already been elucidated with respect to the activities of the NKVD it seems probable that here too they exercise some sort of control. The use by this Commissariat of the one-time additive pad for re-encipherment of its code is exactly the means employed by the RKKA for the re-encipherment of its operational 5-figure Chiffrecode.

C. The Peoples Commissariat for Foreign Trade

The Peoples Commissariat for Foreign Trade also uses an additive pad system for re-encipherment of its communications. In fact each Commissariat has its own code book and the pad system is generally used for the re-encipherment of the external communications passing to or from the head offices in Moscow.

D. The Communist-International

Only in the cryptographic systems of the Comintern for its signal communications with the Communist parties in foreign countries is there an exception in the use of the additive pad, as such, -- here the most essential parts, the keys for the encipherment, are not outwardly to be recognized as cryptographic material, the necessary digit sequences being derived from a book text by means of a mnemonic key. This development corresponds to the introduction by the NKVD of similar systems in their agent organizations and in point of fact one of the functions of the Comintern is espionage, political, economic or military according to opportunity. While little is known regarding the chain-of-command for issue and usage of cryptographic materials in the foreign services of the USSR, the logical surmise is that the NKVD through some of its many organs exercised its usual surveillance.

V. THE BASIC SYSTEMS AS FOUND IN RUSSIAN CRYPTOGRAPHY

A. Substitution Systems

All the substitution systems found by the Germans in the cryptanalysis of Russian traffic are definitely code types. By code is meant not only a substitution system of considerable extent having arbitrary numerical or letter groups assigned as substitutes for the syllables, words and phrases of the language but also those substitution systems of small size which have values for elements in addition to single letters of the language, such as marks of punctuation, the 1-digit numbers and a few short words which are frequent in the traffic of the service for which the table is compiled. It may be noted in passing that the only case reported by the Germans of a true monoalphabetic substitution being used by the Russians, and that without re-encipherment, was between two radio operators in traffic concerned chiefly with women. Evidently it was a personal system being used without authority. These code systems varied in size from small signal tables with 100 groups or less to large books with 25,000 groups or more. They will be classified according to the lengths and types of code groups used in the substitution process, that is, into 2-figure, 3-figure, 2-figure-letter, etc. The original Russian designations will be indicated when known. Details of the various methods of re-encipherment that were used with these codes will be given under a separate heading.

1. 2-Figure Codes

Small signal tables comprising about 100 plain elements represented by 2-digit numbers were used by the Russians to encipher the operational traffic of the army and army airforce from regiment down to platoon during 1935 and until the change in organization of the RKKA which took place in 1942. The original RKKA designation was PT or chatter table. Signal tables of similar construction were used by the NKVD in the communications of their Frontier Troops and Coast Guard Units during the same period, but since the internal arrangements of the vocabularies of the NKVD tables (recovered by the Germans only through cryptanalysis) evidently could not be made to coincide with any of the basic arrangements of those captured in the "PT" series, it is likely that for NKVD usage there was another designation. The PT-35 (chatter table of year 1935) was in use from 1935 to 1939. PT-39 was used during period 1939-42; PT-41 during period 1941-45. PT-42 and PT-43 were also seen.

All these substitution tables, although differing in details of vocabulary, the use of variant readings and switch groups, conformed to the same general pattern. The 100 cells of a 10 by 10 square table were filled, sometimes in systematic order, sometimes in random order, with the 30 letters of the Russian alphabet, the 10 digits 0 to 9, the punctuation marks and the frequent words used in operational traffic. Along both the vertical and horizontal margins of this table the digits 0 to 9 were inscribed in random order as row and column coordinates. Encipherment of a particular word was accomplished by finding it within the substitution table and tracing orthogonally outwards from this cell to the row and column coordinates which were combined to give the 2-figure substitution. The enciphered messages were sent sometimes in

2-figure, sometimes in 4-figure groups.

Sometimes variants were introduced in these tables, that is, each of the high frequency letters of the language would be entered two or more times in the table thus giving a choice of two or more different encipherments for such a letter. Sometimes also two different plain values appeared in the same cell and switch groups were used to indicate which was to be read. While a switch group might indicate one of the meanings, "Take first reading" or "Take second reading", generally the interpretation was, "Read the entire word" or "Read the first letter of the word." In the latter case only one plain value would be inscribed in a cell.

While the internal structure of a table remained unchanged for long periods, the external features or row and column coordinates were subject to frequent changes, the intervals varying from a day to a week or longer. These changes were effected by means of the so-called "system squares" which are merely latin squares of size 10 by 10. The 100 cells of a latin square are filled with the digits 0 to 9 in random order but in such a manner that in each of the ten rows or in each of the ten columns there are always ten different digits. Since such a latin square gives 10 different choices for a row coordinate sequence and 10 different choices for a column coordinate sequence, it is possible through the combination of one chatter table and one system square to generate 100 different substitution tables.

By writing the days of the month along both the vertical and horizontal margins of the latin square a key is provided for the choice of row and column coordinate sequences to be used in conjunction with the chatter table.

All the 2-figure codes of the "PT" series were worked in this way. As regards the actual mechanical arrangement it is a minor detail whether the 100 different substitution tables generated from the combination of one chatter table and one system square were bound in a 100 page book or whether it was necessary to make inscriptions on the margins of the chatter table whenever the coordinates changed. It may be pointed out that all the data may be arranged on one sheet of paper in a square, size 20 by 20, with 400 cells. This lage square is divided into four equal quadrants. The upper left quadrant is the date or key square. If dates are used for keys then it is likely that only 30 or 31 cells of the possible 100 will be filled and the distribution of these dates will be such that generally only three will fall in any one row or column. The upper right and lower left quadrants contain the system square, identical for each of these quadrants. The lower right quadrant is the "PT" or chatter table. Thus the location of a date in the upper left quadrant will indicate on the same horizontal line and in the upper right quadrant the proper column coordinate sequence to be used with the "PT" table directly below in the lower right quadrant. Similarly a vertical line from the date will locate the proper row coordinate sequence. Having selected the row and column coordinate sequences, encipherment of a text proceeds in the manner already explained for the single "PT" table.

In addition to recovering many of these tables cryptanalytically the Germans also captured some of them during

the first year of the war. And although the point is not definitely established in the literature examined, it seems probable that the actual mechanical arrangement was in neither of the ways so far suggested. Instead, it is likely that the "PT" table was issued without inscription of any coordinates on its margins. On the back of this table there would be two pockets for holding the system squares. Two copies of the system square in current use would be issued to each holder. By a vertical folding of the system square and insertion in the pocket at the left margin of the "PT" table, the row coordinate sequence is selected and remains visible at the left margin. Similarly a horizontal folding of the other copy of the system square and insertion in the pocket at the top margin of the "PT" table will provide the column coordinate sequence. Instead of dates to indicate the selection of a combination of row and column coordinate sequences, the system square is reported to have also been keyed frequently by its marginal digits, that is, the digits in the top row of the system square are the keys for the selection of a particular column from this square for use as a row coordinate sequence on the "PT" table, and similarly the digits in the first column at the left of the system square are the keys to indicate a particular choice of a row from this square to be used as a column coordinate sequence on the "PT" table. Following this procedure in the choice of coordinate sequences a two-digit indicator or key was often found by the Germans at the very beginning of code messages.

Methods used by the Russians to generate a new set of row and column coordinate sequences from a basic set were also uncovered by the Germans. These were probably measures of an emergency nature adopted by the Russians during a difficult period in the compilation and distribution of system squares.

It was noted that basic coordinates were sometimes changed by the addition of a one-digit constant to all the digits of a coordinate sequence. Two different constants were generally used, one for derivation of the row coordinate sequence and the other for derivation of the column coordinate sequence. The two constants would be transmitted as a two-digit indicator inserted at the beginning of the code message.

Another way of changing the basic coordinates was by a cyclic displacement of the sequence, that is, by a sliding of it relative to the margin of the "PT" table. A two-digit indicator would be sent at the beginning of the code message, one digit to indicate the starting point in the row coordinate sequence that was to be placed in juxtaposition with the top row of the PT code and the other digit to indicate the starting point in the column coordinate sequence to be placed in juxtaposition with the first column at the left of the PT code.

A still more complicated way of changing coordinates was found to be the derivation of a digit sequence from Russian plain-language or a key word. The letters of a ten letter or longer key word were numbered from left to right according to their sequence in the alphabet. If this derived digit sequence was used unchanged as a row coordinate sequence then a column coordinate sequence was usually derived from it. This was generally accomplished by the addition of a constant or by the use of a substitution sequence. In the latter case, the substitution sequence was probably a row or column selected from a discontinued system square. This substitution sequence consisting

of the ten digits 0 to 9 in random order was written below the digit sequence derived from the key word so that there was an alignment digit by digit between the two sequences. The digits of the sequence derived from the key word were then rearranged in the order indicated by the substitution sequence always beginning with 1 of this sequence and continuing in numerical order through to 10 or 0.

Messages were sent in the PT codes without any re-encipherment. Because of the frequent change in coordinate sequences and the small volume of traffic enciphered using any one combination of coordinate sequences, such additional measures for the security of these communications were evidently thought by the RKKA to be unnecessary at that time. However, it is interesting to note that unsuccessful attempts were made by the NKVD to camouflage its traffic encoded with signal tables similar to those of the "PT" series by the insertion of a null digit between the first and second, the third and fourth, the fifth and sixth, etc., 2-figure code groups. The groups in the transmitted cipher text were therefore 5-figure, the middle digit being the null. Furthermore the null digits were used in numerical order. It is recorded also that the NKVD did in certain instances re-encipher their code messages of the 2-figure "PT" type by means of a transposition system.

2. Variable 1 and 2-Figure Codes

These are very small codes, not monoalphabetic substitutions in the strict sense of the word, since a substitution value is provided not only for each of the 30 letters of the Russian alphabet but also for words, such as "repeat" and the various marks of punctuation. These codes were sent re-enciphered and were intended primarily for the use of agents and partisans since the small signal tables may easily be reconstructed from memory by use of suitable key words or phrases and in fact all the necessary data for encipherment of messages might be based according to agreement on some innocent looking and popular novel.

Great variety was noted in the methods used for constructing these signal tables, especially was this so in respect to the size of the table. Basically the details were as follows:

The 30 letters of the Russian alphabet, the marks of punctuation, and a certain number of other words or 1-digit numbers, according to the limitations imposed by the size of the rectangle, were entered in a mixed order determined by the use of a keyword into the cells of a rectangle of size, say 4 rows by 10 columns, leaving in this case three blank cells according to agreement in certain positions of the first row of this rectangle and completely filling the remaining cells. The ten digits 0 to 9 arranged in a seemingly random sequence, which however was generated in some agreed-upon manner from a keyword, were written across the top of this rectangle as column coordinates. The three digits falling above the blank cells of the first row were used as row coordinates for the second, third and fourth rows of the rectangle. Thus in the substitution process, using a rectangle of above size, seven letters of the alphabet may be represented by single digits and the remaining letters of the alphabet and the words or punctuation marks will be represented by 2-digit numbers which begin with one of the three digits assigned as row coordinates. No matter what digit lengths are used for the transmission of a message, confusion will not result during the redivision of a code text into

substitution units since the three digits agreed upon as row coordinates can never stand alone as substitution units but must be the initial digits of 2-digit numbers in order to have meaning in the signal table. The number of letters to be expressed by a one-digit number generally varied between 5 and 7. Consequently, the number of rows in the rectangle containing letters or words represented by 2-digit numbers would vary and the size of the code would run from 37 to 55 elements.

Generally speaking, messages encoded by means of signal tables of this type were re-enciphered by either a transposition or additive process and the Germans undoubtedly learned of this in the more difficult cases only through the capture of agents. However, the evidence is that non-reciphered messages were also sent in codes of this type and in the cases where this was allowed, provision was made for the very frequent change of the coordinates of a signal table as was done with codes of the "PT" series. In the present case only one new arrangement of the ten different digits is required for a change of coordinates since it is a characteristic of this system that the agreed positions for the blank cells in the first row will indicate the digits in the column coordinate sequence that are to be used as row coordinates.

3. 2-Figure-Letter Codes

Code groups composed of mixed elements, in this case combinations of one digit and one letter, were noted by the Germans in the traffic of certain border guard districts prior to 1939.

The characteristic 10 by 10 signal table of 100 cells was filled in mixed order with the letters of the Russian alphabet, the one-digit numbers, the marks of punctuation and the frequent words or phrases peculiar to the traffic of that service. The signal tables were different for each district and the original NKVD designation is unknown. The method of encipherment is similar to that already noted in the case of the "PT" tables only here we have ten letters of the Russian alphabet in random order as column coordinates and the usual ten digits in random order as row coordinates. These coordinates changed daily, the numerical ones being selected from a digit square and the letter ones from a letter square. It is likely that these system squares were folded and inserted in pockets at the back of the signal table in the manner already suggested for the "PT" tables.

4. 3-Figure Codes

a. The VAK-38

The last general airforce system to be used by the Russians is said to be the VAK-38, Air Force Code of 1938. It was a 3-figure code comprising some 800 groups. The vocabulary contained the letters of the alphabet, words (no syllables), cover groups for airplane types, numbers, marks of punctuation and composite concepts such as "Airplane -------- has made emergency landing" or "Airfield unsuitable for landing."

According to the German description of the system messages were transmitted in either of three basic encipherments

which were designated black, red or green. The 800 plain-elements of vocabulary were arranged in alphabetical order and divided also into 80 decades. Three different dinomes, the black, red and green, were assigned to each decade. The black encipherment by decades had 80 different dinomes (20 of the possible 100 being dropped) and similarly for the red and green encipherments. In each of these color keys the dinomes ran in either an ascending or descending sequence from decade to decade, but evidently no relation could be found by the Germans between these sequences. To each line of each decade three different single digits were also assigned and likewise designated as the black, red and green encipherments. In each color key the ten lines of a decade had the ten digits 0 to 9 arranged in numerical sequence, only in passing from decade to decade the starting points of the sequence were changed with respect to the top lines of the decades. This sliding seems to have been in an irregular manner, that is, when passing from decade to decade in the alphabetical order of the vocabulary. The encipherment of a plain-element was in one color key only and was indicated by the 3-digit group composed of the dinome of the decade and the monome of the line in which it was found in the vocabulary. Only the one color key was used throughout the encipherment of a particular message.

The Germans report that re-encipherments of each of these three basic codes were quite frequent. A re-encipherment was accomplished by a dinome substitution for the AB elements of the groups, the element C remaining constant within the basic encipherment. That is, the Germans imply in their description of the VAK-38 that it consisted of <u>one</u> book only with the three possible readings per element of vocabulary being distinguished from each other by the color of the printing or their position on the line of the vocabulary and that re-encipherments were applied to each of these three basic codes by a <u>second</u> process of substitution from a dinome table. That is, the cryptographic clerk had to remember to keep to the one color key when using the book to encipher a message and then having produced an intermediate text, he imposed on it another substitution process in the classical manner. Evidently the Germans were unable to force a further reduction in the process.

This is a particularly interesting development in view of the trend <u>definitely</u> established for code books of the "OKK" type, namely, re-encipherments were produced by the insertion of dinome substitution tables in pockets at the back of the vocabulary, and a trend also suggested in the use of signal tables of the "PT" type and probably also those of the "SUV" type. But since it has not been established that a copy of the VAK-38 was ever captured by the Germans and in spite of the fact that there is good evidence that substitutional re-encipherments of intermediate texts were performed as a <u>second</u> step by the Russians in a case to be discussed later, it is here suggested that the above description is only based on the results of German cryptanalysis and that the actual operations of encipherment and re-encipherment may not have been as complicated as thought. Three separate and current editions of the VAK-38 may have been involved and these were designated by the Germans as the Black, the Red and the Green VAK-38. If three volumes were actually involved, then it would be a simple matter to work the re-encipherments for each volume by the insertion of dinome substitution tables in a pocket of the vocabulary in a manner similar to that said to have been used for the "OKK" books. While the actual size or format of a page from the

VAK-38 does not seem to be definitely established from the present sources of information, the fact remains that the code is of such small size, only 800 plain entries compared to 5000 for OKK-5, that such a mechanical arrangement can be worked without difficulty.

b. Other Books

Many other 3-figure codes are said to have been used by the Russians although none are specifically described in these sources. The Air Force used many of them for practice in connection with the manoeuvre-like parade on 1 May in Moscow. Starting and landing reports, weather reports, operational messages of the air units arriving from all parts of the Soviet Union to participate in the parade were enciphered with these. For the most part these 3-figure codes were systematic, that is, alphabetic or partially alphabetic as regards the arrangement of the vocabulary with respect to the numerical order of the substitutes. The size of the vocabularies varied from 500 to 1000 elements. The vocabularies generally contained entries for all the letters of the Russian alphabet, the frequent bigrams, the marks of punctuation, the prefixes and suffixes characteristic of the language, the frequent words peculiar to a particular service and the numerals. Changes in encipherment are said to have been made in a manner similar to that used on the 2-figure codes, only in this case it was a "single digit substitution" for the elements A, B and C. These elements were probably the numerical designations for the page, the line on the page and the column on the page where the plain reading was to be taken. The evidence indicates that while the re-encipherment process is equivalent to the use in rotation of three different 10-digit substitution sequences, in which case all first digits of the 3-figure groups of intermediate text will be re-enciphered from the same substitution and a particular digit whenever it occurs in this first position will take as a substitute only the single value, it was probably accomplished by the interchange of various substitution tables at the margins of the vocabulary. In the present case it can still be done by the use of only two tables and this is generally true for all vocabularies of 10,000 elements or less and provided of course that the re-encipherments are confined to the use of monome or dinome substitution tables which are always used in phase with the elements of an intermediate code group AB, ABC, or ABCD.

From the present sources of information it is difficult to pin the use of a certain method of re-encipherment to any particular code book. Without doubt "additive" methods of re-encipherment were also used on all these small codes, 2-figure, 3-figure or 4-figure. Alex Dettmann dates the introduction of "additive" methods for codes of this type to the year 1940. Doubtless both "conversion" tables and "additive" were used side by side. The discussion of any methods of re-encipherment which actually do require a second step or process has been left for a separate heading.

5. 4-Figure Codes

a. The "OKK" Books

Codes of the 4-figure type containing around 5000 groups and oficially designated as "OKK", General Commander Code, were first used by the Russians in connection with manoeuvres in the Volga military district and various editions

continued to be used for the encipherment of the communications of army, corps, and division until 1941. It is said that such extraordinary technical skill was shown in the compilation of OKK-5 that its successors needed only slight changes as regards choice of vocabulary. The swift succession of four great codes in the course of the years 1939 to 1941 is explained only by the fact of their capture -- "OKK-5" in the Finno-Russian war, "OKK-6" to "OKK-8" in the German-Russian war. All these codes with the exception of OKK-8, however, had been recovered analytically and were being read currently by the Germans before their capture.

The Germans seem for some time to have been under the impression that a re-encipherment was being applied to a basic 4-figure code book, one dinome substitution table being used for the elements "AB" and another dinome substitution table for the elements "CD". But the evidence seems to be that the Russians achieved this effect and avoided the extra operation of an actual re-encipherment by means of a very clever arrangement of pockets for insertion of dinome tables in the covers of an unpaginated book containing only the vocabulary, a trend which has already been suggested in the discussion of the actual format of the "PT" table and its component, the "system" square.

While a copy of an "OKK" book is not available for proof and although the meaning to be taken from the English translation of the description in German is obscure on some points, the following description of OKK-5 is thought to be an accurate interpretation and typical of this series.

The vocabulary is a book of 50 pages with 100 plain groups per page. Each page has 25 lines so that there are 4 columns of 25 plain groups each to a page. These groups are arranged in alphabetic order and consist of letters, syllables, words, phrases, the numbers from 00 to 99, marks of punctuation, cover names for plane types as well as a few reserve cells for additional entries. The pages of the book are bound along the bottom margins and printed on one side only, that is, it is an end binding rather than a side binding. No numerical references are to be found either as paginations or as column or line indicators in this book. However, the pages do show letter indices not only for purposes of easy reference to the vocabulary but also for a more important reason which will be presently clear. The first 25 pages show positional letter indices at the right margins and the last 25 pages have them at the left margins. These 50 different indices, probably the initial letter or letters of the first word on a page, are distributed over the 25 lines per page of both the right and left margins so that the position of an index uniquely determines a page. The margins are cut to varying depths to provide a visible index system.

Instead of assigning numerical code groups to the elements of the vocabulary in the orthodox manner it is now possible to work a clever mechanical arrangement whereby a completely new random repagination may be obtained whenever desired without going through the second step of a re-encipherment by conversion tables as has often been done in the past. A pocket is attached to the inside of the back cover of the book so that two dinome substitution tables may be inserted, one overlapping the right margins and the other overlapping the left margins of the pages. When the tables are correctly folded and inserted in their pockets two columns of 25 dinomes each will be visible against the right margins of the pages

and two columns of 25 dinomes each likewise visible against the left margins of the pages. That is, when the book is opened at any given page, four different dinomes will be visible at each line, two at the right extremity and two at the left extremity. Since we have 100 positions for vocabulary on a page or 4 columns of 25 and 100 different dinomes visible at the margins, also 4 columns of 25, it is possible to indicate uniquely a plain group on a page by the position of a certain dinome in a particular alignment of the two dinome substitution tables with respect to the basic vocabulary. Furthermore the page may also be uniquely determined by either of the two dinomes standing immediately opposite the index letter on that page. Thus any plain group in the vocabulary may be represented by a 4-digit code group, the first two digits of which indicate the page on which it is to be found, and the last two digits the line and column of that page. In addition, since there are only 50 pages in the vocabulary and a distribution of the 100 different dinomes so that two stand immediately adjacent to each page index, two variant page readings are possible at each substitution.

The dinome substitution tables when unfolded have a width of about 18 columns and a depth of 50 lines. Only the dinomes 00 to 49 will appear on the left table and only those from 50 to 99 on the right table. The margins of these dinome tables will be indexed in numerical order. If the numbers from 00 to 24 are used as indices to the columns of the left table then the numbers 25 to 49 will be the indices for the lines of this table, the latter consecutive numbering being repeated twice since there are 50 lines. Similarly the numbers from 50 to 74 will index in numerical order the columns of the right table and the numbers 75 to 99 in numerical order and repeated will index the 50 lines of this table. These marginal indices serve as indicators for the folding and placement of the dinome tables in the pocket of the book prior to encipherment or decipherment of a message. A 4-digit indicator is sufficient for the correct placement of each table. Thus the indicator 1135 means that the left table is to be folded in such a manner that when it is inserted in the pocket of the book column 11 will be immediately adjacent to the left margins of the pages and line 35 is in alignment with the top line of the vocabulary. Similarly for a placement of the right dinome table.

Because of the limitation on the block of dinomes that may appear internally in each column of these tables, the process of deciphering is not too laborious. While only dinomes from 00 to 49 may appear on the left table, those in the block 00 to 24 will be confined to the odd numbered columns and those in the block 25 to 49 to the even numbered columns. Each column will have its 25 different dinomes arranged in a random order and the sequence will be repeated to fill the 50 lines. There is no relation between the sequences of dinomes in the various columns. That is, the table is completely random within the above limitations. In the same way the odd numbered columns of the right table will have in random orders only dinomes from the block 50 to 74 and the even numbered columns those from block 75 to 99. Thus it follows that a selection of any two consecutive columns from the left table combined with a selection of any two consecutive columns from the right table will contain only the 100 different dinomes 00 to 99 which is the condition for uniquely indicating each of the 100 positions on a page of the vocabulary and also for uniquely indicating in a twofold manner each of its 50 pages.

The positions of the dinome substitution tables relative to the code book were changed from message to message and such changes were indicated by two 4-digit indicator groups which were generally sent at the beginning of the cipher message. Messages were also sometimes sent without indicator groups which means that on certain nets the choice of indicator was definitely subject to regulation according to a prepared table and that in all probability an attempt was made to prevent the overloading of an indicator with traffic by careless cryptographic clerks.

While the code book remained unchanged for a long time unless there was a physical compromise, new dinome substitution tables were issued frequently. In some areas they were changed daily. Of course different substitution tables were required also for each crypto net.

Another 4-figure code similar to those in the OKK series as regards structure and method of encipherment was the OSKK-7, General Central Commander Code - 7. It was the so-called railroad and communication code for rear area liaison and yielded very valuable hints regarding supply and new formations of the enemy. It also was captured at the end of 1941.

b. <u>The SUV Tables</u>

Another type of 4-figure code used by the Russians was the system designated as SUV, Camouflaged Communications of the Command. As already pointed out, signal tables of this type were introduced by the RKKA at the time of the decentralization in 1942 of the production and issue of systems to be used at the front. Great latitude was given individual fantasy and initiative through the fact that the signal officers of every division, indeed of every regiment, were able to compile and develop their own systems for their own areas.

The use of switch groups to indicate a change in reading, that is, "read the first letter of the word" or "read the entire word", first noted in the later "PT" tables was retained in the compilation of these "SUV" tables and represented very considerable advances in security in comparison with the earlier small substitution systems. The characteristic format for these codes was outlined in a general way by the 8th Section of the General Staff in Moscow. With the decentralization in production and issue of these signal tables it is not clear whether the trend was maintained of providing pockets at the back of the chart for the insertion of substitution tables as noted for the "PT" and "OKK" systems. It is certain that new tables were compiled frequently and it is possible that changes in coordinates were effected by the individual users making their own notations or preparing their own strips. Since the use of a particular signal table was confined to a very small area, distribution was no great problem.

These tables were frequently of a size 20 rows by 10 columns. The 200 cells of the table were filled with Russian words and phrases in partially alphabetic order, that is, words with the same initial letter were grouped together with a few exceptions. Aside from the most important words used in the specialist branch of the service for which the code was compiled, the table contained also the one-digit numbers, the most important marks of punctuation, the switch groups, and the letters of the Russian alphabet.

Three types of coordinates were inscribed on the margins of this table:

(1) To the column Ten different 2-digit numbers were selected and assigned in random order, one to each of the ten columns of the table.

(2) To the double row The ten different 1-digit numbers were assigned in random order, one to each of the ten double rows of the table.

(3) To the single row The ten different 1-digit numbers were assigned in random order, one to each of the top ten rows of the table. This digit sequence was repeated again assigning one digit to each of the ten bottom rows of the table. A variant reading for each of the twenty rows was now generated from this basic sequence by adding in modulus 10 the same constant to each of the twenty 1-digit numbers.

Encipherment of a particular word or phrase is by means of a 4-digit group produced by reading the coordinates of the cell in which the word is found in the order: column (the dinome indicating the column in which the word is found); double row (the single digit indicating the double row in which it is found); row (one of the two single digits which indicate uniquely the particular row of the double row in which it is found). Thus a word may be represented by either of two 4-digit groups. Additional variants are also often produced by assigning several different 2-digit numbers to each column of the table, and in theory since there are in all 100 different dinomes, ten variants per column are possible. While there is no indication that the Russians did make use of such a great number of variant readings for a plain element, there is evidence that the size of these signal tables varied some containing as many as 2,000 plain elements in which case full use would be made of the 100 different dinomes.

In connection with the above description of a basic 20 by 10 signal table it should be noted that it is just as effective and probably more efficient to assign ten different dinomes at random as coordinates for the 10 columns and twenty different dinomes (or forty with two to each row) also at random as coordinates for the 20 rows of the table. And in point of fact that is exactly the method followed by the Russians in many of their 4-figure SUV systems, encipherment by dinome substitution for elements AB and CD. The system as originally described may also be worked in this way regardless of the limitations noted for the element D of the CD dinome substitution. Using the latter method as a point of departure it is conceivable that the 8th section of the RKKA in Moscow fixed the size of the chart or table to be used on a certain type of crypto net together with the choice of vocabulary. Blank tables of the given size would be supplied in quantity and it was the function of the competent cipher authority to vary the internal arrangements of this vocabulary in the table according to his own fancy whenever making a new compilation. Pockets might also be provided at the backs of these vocabulary tables and it would be the further function of the proper cipher authority to compile his own AB and CD dinome substitution tables for insertion. If the CD table is to provide row coordinates and there are 20 rows

to the vocabulary then it is only necessary that 20 different dinomes at the least be arranged in random order for any particular column and the series may be repeated to a depth of 40 rows to allow for a variable placement of the dinome table. CD tables with 40 rows would allow not only a change to new coordinates but also a sliding of the same coordinates with respect to the vocabulary. Similarly dinome tables for the AB substitution or column coordinates are compiled, the requirement being that at least 10 different dinomes be arranged in random orders in the rows of this table. The placement of these dinome tables relative to the vocabulary might be indicated in a manner similar to that used for the OKK series. No evidence was found to support this theory regarding the mechanical operation of the SUV systems, but in view of the trend already noted it is suggested that it is more than a possibility.

Since in general addresses and signatures spelled out in letters or syllables afforded the most important starting points for cryptanalysis, the Russians began in 1943 to encipher these addresses and signatures in messages in the SUV systems with special address and signature codes which in addition to names contained also expanded concepts such as "commander of the 17th tank brigade". The Germans found interpretations of this type very difficult to reach and they were only risked after a very careful and intensive study of the traffic involved.

In connection with these "SUV" tables it should be pointed out that SUV, Camouflaged Communications of the Command, seems to be a general term applicable not only to the 4-figure codes here described but also to the 2-figure or 3-figure codes of types already discussed provided that they were compiled by signal officers of the RKKA for use in the lower echelons of their own area. The term was introduced under 4-figure codes since the majority of such signal tables were of the 4-figure substitution type. Instead of being assigned to particular code types, the term is better used as indicative of a certain critical period in the security of the communications of the RKKA. On the other hand, the terms "PT", "OKK", etc. are the correct designations for codes issued in a specific series by a centralized authority.

c. Other Books

Another Russian 4-figure code, the first general airforce code in use from 1935 to 1937 was likewise characterized by several reencipherments and doubtless this was accomplished mechanically by the insertion of dinome substitution tables, in this case only one table being used at a time, in a pocket at the back of the book. The original Russian designation is unknown.

According to the German description based presumably on the results of analytical recovery, the book consisted of ten pages with provision for the entry of 100 plain elements per page. The vocabulary was arranged in strictly alphebetical order and the cells on each page were numbered consecutively from 00 to 99. For pagination, dinomes were assigned to each page in an irregular manner, as many as ten different variants being permitted per page. Encipherment was accomplished by reading in order: selectively one of the dinomes of the page

involved and the dinome indicating the position of the plain element on the page. Reencipherments were confined to repaginations, being changed randomly on each crypto-net as deemed necessary.

Many other Russian 4-figure code books were worked on by the Germans from 1935 until the end of the war. Deltmann gives a very interesting account of how one of the NKVD codes was broken. It was a 4-figure code of some 25 pages with 100 groups to the page reenciphered with a dinome substitution table which changed approximately every week. It was being used from 1935 on in the border guard district of Kazakstan where the troops were often isolated in winter due to frequent distrubances of telephone and telegraph wires by snowstorms. It seems that news reports were often received in this code and that early in 1936 a speech by Stalin which had been printed in "Pravda" and in "Red Star" was transmitted to the border units of Kazakstan by radio as a cipher message. This message, some 1800 groups long, was recognized as having been enciphered by a code which had not yet been extensively broken and the content was soon identified by samples as that of the printed speech. Thus was a very imperfect knowledge of the code materially expanded by the Germans.

Typical of the NKVD 4-figure codes is the one known as "ZERNO" being used by some Russian Border Guard and Security Troops at the time of the German capitulation. The book consists of 50 pages with 50 plain elements per page. The vocabulary is arranged in alphabetic order. It contains the letters, digraphs, trigraphs, syllables, words, numbers from 0 to 31 corresponding to day dates, marks of punctuation with variants and cover groups for surnames of military and political leaders (differing in each net). The pages 01 to 50 and the lines 01 to 50 of the basic code are each enciphered by two different dinominal substitution sequences. Each page and line of the basic code can therefore be expressed in two different ways thus giving a choice of 4 variant readings for each plain element since the 100 different dinomes are available for only 50 pages and also for 50 lines of the basic code. It is quite probable that two dinome substitution tables are folded so that two columns of dinomes remain visible on each table when they are inserted in pockets at the back of the book in a manner similar to that noted for the OKK series. ZERNO was used on more than 30 different nets and each net had 20 substitution tables for reencipherment, 10 each for the page and the group.

It is not clear how Alex Dettmann knows that the original Russian designation for this code is ZERNO inasmuch as it was still in use by the NKVD at the time of capitulation and he is quite definite in the claim that no live cryptographic materials used by the NKVD were ever captured by the Germans.

Two other 4-figure codes used at this time by the NKVD Border Guard and Security Troops are reported to be "NIVA" and "VIZA". "NIVA" is said to be reenciphered by two dinome substitution tables and "VIZA" by a dinome and mononome substitution. In the latter case one digit of the 4-figure code group evidently remains unchanged during the various reencipherments.

6. 5-Figure Codes

a. The Chiffrecodes

For the transmission of radio messages of operational content, that is, dealing with troop command on the nets of the upper and top command (from brigade or division staff upward to the General Stff of the RKKA) the 5-figure "Chiffrecode", also called "Operational Code" was used. The "Chiffrecode" was systematically adapted by the Russians in the course of years to the changing requirements of their vocabulary and was improved in respect to security against cryptanalytic attack by more and more consistent use of variants for the most frequent groups. These new editions of the "Chiffre" came during the war at intervals of 6 to 12 months, whereas in peacetime the same code was used much longer. At the beginning of the German-Russian war code "011-A" was in use which was then replaced by Code "025-A", "045-A", "062-A" and finally by code "091-A" which remained in use until the capitulation of Germany.

All these codes, except "045-A" which was in use from March 1942 to March 1943, were alike in structure -- aside from the above mentioned progressive improvements and amplifications. They were divided into the general part with vocabulary in terminologic-alphabetic order and the "special part". The general part contained letters, digraphs, trigraphs, syllables, words, phrases, and entire sentences arranged in strictly alphabetic sequence, with the marks of punctuation, fractions and ordinals, hours and minutes, numerical designations of armies, corps and divisions, day dates, year dates, and calibre designations scattered throughout the entire code. In the special part these concepts, which had been entered out of alphabetic order, were brought together once more in numerical order to facilitate looking up these concepts in the code by the code clerk. Code "011-A" embraced some 19,000 groups which were entered on some 390 pages; the systematic development of the code resulted in an increase in the number of groups with each new edition. The last known code "091-A" had some 23,000 groups on 430 pages. The number of variants increased with each new edition of the code and in the final edition "091-A" reached a total of some 230 groups for each of the two marks of punctuation, period and comma.

The code "045-A" fell out of the ranks of the terminologic-alphabetic codes. It showed interrupted alphabetic structure. It is interesting to note that, while all new versions of the Chiffrecode during the course of the war were always captured by good fortune so early that the originals were almost always in the hands of the cryptanalyst by the time they were put into use by the Russians and consequently there was no necessity for code recovery, precisely the more difficult code "045-A" did not fall into German hands until some three months after it had been put into use in the RKKA. In these three months, however, it had been so far recovered by the German cryptanalysts, in spite of the essential departure from the structure of its predecessors, that they were reading currently parts of the messages encrypted by it.

Messages encrypted in these codes were always sent reenciphered. And there is no question here regarding the method. "Conversion" tables were never used; it was additive and frequently a one-time pad.

b. Other Books

A 5-figure code of another type was also recovered analytically by the Germans. It was a major substitution system of the NKVD organs used in connection with railway transportation, and was still active on the day of German capitulation. The code contains 2500 groups on 25 pages with the elements AB and DE of the 5-digit group ABCDE each being enciphered by a dinome substitution sequence and the element C by a monome substitution. With 25 pages of 100 groups each, it was possible to express every meaning of the basic code in several ways in an encipherment and thus prevent repeats. For each of the 25 pages (AB), 01 to 25 in the basic code, there were 4 possible choices with 100 different dinomes (00 to 99) being available within an encipherment. The middle element C divided each page into 4 quarters and indicated the quarter used. Consequently with 10 digits (0 to 9) two quarters could be expressed in 2 ways and the other two quarters in 3 ways. There were then either 8 or 12 different ways of expressing the same basic code group in any encipherment. According to the German description the expansion of variants ended here. But since there are only 25 lines of vocabulary to each quarter, it would have been possible to have likewise 4 choices of dinomes for the line or DE part of the substitution. Although the point is not made clear it is quite likely that the whole 100 dinomes were used to indicate the DE substitution, that is, one to each of the 100 elements of vocabulary on a page, since this feature would be a great aid in the correction of those corrupt groups which are often present in radio traffic.

It is clear that three "conversion" tables are used, two dinome substitution tables and one monome substitution table, and that these must change frequently to provide the numerous reencipherments so characteristic of small Russian codes of this type. It is here suggested that these reencipherments were done mechanically in one step by the juxtaposition of tables with the margins of the vocabulary.

7. The Methods of Reencipherment

a. Methods Which Require a Second Step

As already indicated in this paper various methods of reencipherment were applied to the basic 2-figure, 4-figure or 5-figure code books used by the Russians. In some cases there has been the question as to whether a second step or process was actually involved. We have consistently favoured the simpler interpretation whenever possible since the evidence seems to indicate that one and one authority only has been responsible for the compilation of cryptographic materials and traces of a certain physical similarity in these materials have been indicated. Thus, a complicated method of reencipherment using conversion tables has often been explained as involving only one step when it can be worked in two steps. Only methods of reencipherment which actually require a second step will be described here and the use of the conversion table, the additive sequence and the transposition to obtain reencipherments of intermediate text in the basic 2-figure, 3-figure, etc. code books will be noted.

b. Conversion Tables

An examination of the available material has revealed the use by the Russians of conversion tables, as a second step in the reencipherment of intermediate text, in only the one instance. They were used with the first general NKVD code, a 4-figure code of 10,000 groups introduced in 1939. This system is said to have been used by all border guard districts or frontier troops of NKVD, the interior troops of NKVD and by other NKVD organs whether military or political. The conversion tables seem to have been used only for a short time and were replaced by additive sequences.

The reencipherment is accomplished in three phases by use of three different 10-digit substitution sequences. These sequences may be arranged in an enciphering table in the following manner: In line 1 are the digits 0 to 9 in numerical order; in line 2 are the digits 0 to 9 arranged this time in random order; similarly for lines 3 and 4, the random orders in each case being different so that there are three different substitution tables. The reencipherment of the 4-digit intermediate text proceeds as follows: In phase 1 of the reencipherment, the digits which are found in positions 1, 4, 7, 10 etc. of the intermediate text are looked up in line 1 of the enciphering table and the substitutes found directly below in line 2 of the table; in phase 2 of the reencipherment, the digits in positions 2, 5, 8, 11etc. of the intermediate text are located in line 1 of the enciphering table and the substitutes taken from line 3 of the table; similarly in phase 3 the substitutes for the digits in positions 3, 6, 9, 12 etc. of the intermediate text are found in line 4 of the table still using line 1 as the reference. Since three substitution tables a, b, c are being used in rotation for reencipherment of a 4-figure code group, such a group can have only three variants according to the patterns abca, bcab, and cabc. Evidently the Russians were not long in evaluating the defects of such a system of reencipherment and soon turned to the use of additive.

c. Additive Sequences

In the additive method of reenciphering the basic 2-figure, 3-figure, 4-figure or 5-figure codes a long digit sequence is added by addition in modulus 10 to the intermediate code text to produce the cipher text.

These additive sequences may be classified according to their lengths, methods of use, and methods of generation. The Germans divided them into five different types, the table, the pad, the tape, cross-addition and the key-book.

The Table

This is an additive sequence of very short length which was used for the reencipherment of messages in the small signal tables already described. It is impossible to pin the use to a particular code, area or time. However, it is said that these tables were used with all the small codes, 2-figure, 3-figure or 4-figure.

A table contained 130 five digit groups arranged in thirteen lines and ten columns. The distribution of the digits in a table was random. The lines of a table were numbered serially from 00 to 12 and the columns from 1 to 0.

This numbering made it possible to begin the reencipherment at any desired point in the table. The starting point, the five-digit group in the table which was to begin the additive sequence, was announced to the recipient by a 3-digit indicator consisting of the line and column numbering. If the starting point lay toward the end of the table, the remaining 5-digit groups frequently did not suffice to recipher the entire intermediate text. In such a case the recipherment was continued beginning with the group in the first line and first column of the table. The five digit groups were taken from the table in normal order, by lines and from left to right.

The tables, called Gamma, are said also to have varied in size, some having been seen with 60, 80, 100 and 120 five-digit additive groups. The periods of validity for these tables are not known.

The Pad

This gives an additive sequence without repetition of much greater length than is provided by the table. A table or Gamma table as the Germans called it, consists of one page whereas the pad or "Bloknot" is made up of several pages or Gamma tables.

The pads likewise served for reenciphering basic code books or signal tables. They seem to have been used for the traffic of a front staff with its associated army staffs or of an army with its divisions and brigades.

The sizes of these pads also varied. One type consisted of ten pages, each of them being a table of 10 by 10 five digit groups. The lines of each page were numbered serially, the lines of page two being considered a continuation of the lines of page one, and so on. The numbering of the lines therefore began with 00 (the first line of page one) and ended with 99. The columns of each page were all numbered serially from 1 to 0.

The recipherment of the intermediate text was accomplished in the same manner as with the table, proceeding from the bottom of one page to the top of the next when necessary. The starting point was likewise determined by a three digit indicator group imparted to the addressee.

These pads or "Bloknots" may also be divided according to the manner of their use into two categories: First, the general pad which was used in the dispatching of messages the content of which was to be available simultaneously to several recipients. A table of the general pad could be used several times, since security was afforded by the use of different starting points. The period of validity, however, for a table of the general pad was only one day. Second, the individual pad which served merely for communication between two partners, the army and one of its divisions, the front staff and one of its armies, etc. A table from the individual pad was used only once, that is, it was a one-time pad.

The general pad used for the reencipherment of messages in the "Chiffrecodes" is said to have contained 31 tables, each table containing 300 five-digit additive groups.

At the top and at the side of the table are entered 2-digit column indicators and 3-digit row indicators which allow the encipherer to indicate according to the principle of coordinates the additive group with which he begins his reencipherment. Hence in general tables reencipherment can start at any point in the table but must then continue serially (probably from page to page) until the last text group has been reenciphered.

The individual pad used with the Chiffrecodes" is supposed to have had 50 tables. Here the sizes of the tables seem to have varied from 60 to 120 five-digit groups. This variation was probably according to the requirements as regards message lengths in a particular branch of the service, since a table was used only the once and the starting point for reencipherments was always the first additive group in the table.

It is interesting to note that these Bloknots were bound in a special way. In an outer covering of thick wrapping paper the sheets or tables were held together on the left side by perforating them and drawing through the holes a string the ends of which were provided with a leaden seal with the impression of the General Staff. This was done in such a way that each single sheet was enclosed in tissue paper in such fashion that only by tearing the tissue paper could the first sheet be released while the other sheets remained sealed. Whenever a new sheet was used, a notation had to be made on the inside of the cover. The sheets were numbered serially 01 to 50. The entire block likewise had a 5-digit number which was printed on the outside of the cover. There was also imprinted the type of the block, individual or general. In addition the pads had a notation usually in ink indicating the formation by which the block was to be used or the area, for example AKORD (army-corps-division), FAK (front-army-corps), OC (special) and CIRCULAR. The designation CIRCULAR seems to indicate that while the pad is a general pad in the sense in which the term general has already been defined it also has a further limitation as regards the area of use, for instance, in the traffic of the army with subordinate divisions and brigades. Only the addressee can decipher a message enciphered by individual additive pad; on the other hand there are always several holders of a particular circular or general pad and each one of these will be able to decipher a message so enciphered.

In connection with the use of the so-called Gamma tables and Blocknots by the Russians it should be mentioned that Alex Deltmann dates the introduction of additive sequences to 1940 and he speaks of the use of "single" additive until the end of 1944 and the use of "double" additive from then to the day of the German capitulation. Evidently the German meaning was either unknown or obscure to the translator. It is here suggested that the correct interpretation is as follows: Before 1944 the 5-digit groups forming the additive sequence could be taken from the table or pad in only one way reading them in the normal order from left to right on the line and the lines from top to bottom on the page, regardless of whether such an additive sequence was used one time or several times for the reencipherment of messages. After 1944 alternative methods of taking out the 5-digit groups from a table or pad to form the additive sequence were introduced, such as, reading vertically, alternating the direction when passing from line to line or column to column or even reading diagonally.

The Tape

In order to avoid the misuse of an additive pad by cryptographic clerks either through the overloading of it with traffic by a careless selection of starting points or the neglect to destroy a page of the one-time pad once it had been used, the Russians evidently have evolved a very clever device which the Germans called a "Morse roll". Five-digit groups were printed in totally unsystematic and random manner on a tape. Two identical tapes were printed, one for each user, and an identical numerical designation given to them. These tapes were supplied to the users in the form of rolls. Here the starting point could not be selected; but was always the first group on the tape. A sufficient length of tape was unwound or drawn out of the device for the reencipherment of the message. Reencipherment proceeded in the usual manner by addition in modulus 10 of the five-digit groups of the tape to the numerical groups of the intermediate text. When the entire intermediate text had been thus reenciphered with the five-digit groups from the roll, the tape was cut after the last five-digit group used and the used portion of the tape was destroyed. The receiver had to do the same thing after deciphering. It seems quite likely, although there is no such indication to be found in the German description, that the device was constructed in such a manner that once the tape was withdrawn it could never be pushed back and would always have to be destroyed.

It is said that a cipher text enciphered by means of this system began and ended with a five digit indicator group, usually not enciphered, consisting of the number of the roll (three digits) and the group count of the message (two digits) less two (two indicators).

It is obviously impossible to pin the use of the additive tape to any particular code book or signal table. It is reported to have been used by the NKVD partisan, scout or agent traffic and this could only have been known by the Germans through capture.

Cross-addition

The case of so-called cross addition is a method of self-generation from the intermediate text. In the simplest form, the intermediate code text was transformed into cipher text by prefixing to it any desired digit (1 to 0) and adding this in modulus 10 to the first digit of the intermediate text. The resulting one-digit sum was entered. This resulting digit was used in its turn as addendum for the second digit of the intermediate text. This addition yielded another sum which was entered and used also as addendum for the third digit of the intermediate text. The sums of such additions to the entire intermediate text, each consisting of a single digit, when taken in sequence constituted the actual cipher text. The digit which served as addendum for the first digit of the intermediate text was prefixed to the cipher text and so transmitted to the addressee.

In deciphering the process was similar; the first digit of the cipher text was subtracted in modulus 10 from the second digit, the second digit of the cipher text from the third, the third from the fourth, etc. This gave the intermediate text which was transformed into plain text in the usual manner by means of the code book or signal table.

This is obviously a very simple method of using the additive process in reencipherment and adds very little to the security of the intermediate text. Various other methods ranging from the simple to the complex were used by the Russians to generate a long additive sequence given one or two 5-digit key groups. The following description is typical: Two different 5-digit key groups are given which we shall call A and B. Then the 1st additive group will be of the form 2 times A plus B; the 2nd is 2 times A plus 2 times B; the 3rd is 3 times A plus 2 times B; the 4th is 3 times A plus 3 times B; the 5th is 4 times A plus 3 times B, and so on. It is understood that while this is the fundamental reduction, the actual process of generation consists of successive additions in the series A and series B using of course addition in modulus 10.

Such systems of cross-addition to generate an additive sequence were found by the Germans in the traffic of the partisans and bands and the self-generated additive sequence was used for the reencipherment of the small 1- and 2-figure code or signal table already described. Thus it was possible to reproduce the cryptographic materials as needed from a mnemonic key.

The Key-book

In this system the additive sequence is generated from Russian plain-text, using for this purpose some popular novel. When the method is used by Russian agents, the choice of book probably conforms to the language of the country in which operations are undertaken. To the ten digits 0 to 9 are assigned the letters of the alphabet. The 25 to 30 letters depending upon the language in which the key book is written are distributed over the ten columns of the table by means of a mnemonic key. Thus a substitution table is prepared so that starting at an agreed point in the book the plain-text may be converted into a digit sequence. This derived digit sequence is then used in the usual way for the reencipherment of messages in the various code books or signal tables.

The Germans were able in many cases to trace these non-random additive sequences to the actual key book. Thus the "History of Leninism" by Stalin is said to have been the basis for the additive sequences used for a time in 1940 for the reencipherment of a 4-figure NKVD code.

d. Transpositions

According to the Germans transposition methods were also used by the Russians to recipher messages encoded by means of their small signal tables. The following method is said to have been used by the border guard Transcaucasus. The intermediate text is produced by means of "system squares" and a signal table similar in structure to the "PT". This intermediate text is divided into sections containing five 2-digit groups. Within these sections the tens of the five dinomes are combined into a 5-digit group and then the units are combined into another 5-digit group in like manner. A further transposition is now applied using this time the ten digits of a section as the unit. The digits of each equal length section have been transposed according to the same pattern and then the sections themselves have been transposed into a new order.

8. Indicator and Discriminant Groups

As regards the use of discriminant groups, that is, the insertion within the body of the cipher text of a group to identify the particular cryptographic system being employed, no mention has been noted in these sources. A distinction by means of the division of the cipher text into 2-digit, 3-digit, 4-digit or 5-digit groups has been found. For instance traffic based on the PT tables was often sent in 2-digit groups whereas that enciphered by means of the Chiffe-codes was sent in 5-digit groups.

On the other hand there seems to have been an extensive use of indicators to signal the starting points on an additive sequence or the choice of a reencipherment. In the case of the additive methods of reencipherment, the indicators themselves were generally enciphered except when the tape or morse roll was used as has already been mentioned. The use of a separate additive table to encipher these indicators has not been noted, but instead certain groups of the cipher text itself have been used. Thus the use of a control group to indicate the choice of an additive group from a table to encipher these indicators has not been found, but the use of a control group to indicate the groups of the actual cipher text which are to be used as additive to either encipher or decipher the indicators has been seen. Thus the final group ABCD of cipher text may indicate such choices. A plus B gives the position of the first group and C minus D the position of the second group to be used. Both indicator groups when deciphered would be identical, one serving as a check on the other. The control group would be part of the actual text whereas the indicator groups would be inserted groups. The indicator group almost always consisted of five digits and was found twice in the cipher text, once at the beginning and once at the close. Whether a control as mentioned above was used on this 5-figure traffic or only on the 4-figure traffic is not clear. The first three digits of the five-digit indicator generally gave the starting point on the additive sequence and the last two digits the data on the numbering of the substit-ution, that is serial number of Gamma table or Bloknot, when this was subject to change. Where the numbering of the substitution was dependent on the date, the indicator contained the starting point for the additive and the date. When the numbering of the substitution remained constant, then the indicator, which contained the starting point for the additive, was filled out with the group count for the message, less the number of indicator groups. The indicator at the close of the cipher text was identical with that at the beginning, that is, when deciphered.

More rarely two indicators were found at the begin-ning of the cipher text, but this only happened when a five-digit indicator was not adequate to impart to the addressee the starting point of the additive and the numbering of the substitution. Unenciphered indicators were also noted in other positions. For instance, the 5-digit serial number of the Bloknot in the second position and the 5-digit indicator (first three digits of this indicating the line and the last two digits the column of the pad) in the third position.

The indicators were often enciphered within an individual circuit by the cipher text standing at a specified position (addition was more usual than subtraction). This was done with both indicators, that is at the beginning and at the end of the cipher text. If for example the indicator at

the beginning had been enciphered with the fifth five-digit group of the cipher text by addition, then correspondingly the indicator at the end was enciphered by addition of the fifth group from the end.

9. Machine Methods

a. The Teletype

According to the TICOM sources, traffic between Moscow and the high staffs at the front was sent by means of a Russian Baudot teletype scrambler. It seems that In 7/VI, a subsection of the Signal Intelligence Agency of the Army High Command (OKH/GdNA) which was engaged in security studies and mathematical cryptanalysis, collaborated with the experts from the Forschungsamt (Goerings "Research Bureau") in the analytical solution of this traffic. The Forschungsamt seems to get the credit for reading this traffic, since Wilhelm Fenner, the former chief of cryptanalysis of the Signal Intelligence Agency of the Supreme Command German Armed Forces (OKW/Chi) said in interrogation that, "the Forschungsamt appears to have been more successful than prejudiced opinion readily admits".

The Forschungsamt in 1943 succeeded in reconstructing a cipher machine on which this traffic was based. The break-in was due to a peculiarity of the machine consisting in the fact that currently compromises seven characters in length were produced. In each transmission pause seven characters of pure key are transmitted automatically before the cipher mechanism is switched off. If no text is sent within these seven characters the first plain letter starts the cipher device operating again. The deciphered text yielded a plain 5-figure code.

b. The K-37

Space does not permit (the sources in any case are none too adequate) that details of the Russian cipher machine, the K-37, be given in this paper. Suffice it to say that no traffic was ever observed by the Germans up to the day of capitulation as being enciphered by means of the machine. The Germans did capture a specimen of the K-37 in 1941 and it was known by them that it was intended for the encipherment of traffic from Army Corps upward. The machine is of the type known as the "Large Hagelin". That is, it was probably built from the Hagelin patent and corresponded to the French B-211 with certain changes. It was so well built throughout and the construction of such mechanically clean work that the Germans were of the opinion that the device could not be of Russian manufacture. One vital part was missing from the captured specimen of this machine. Research on it was done by OKH, IN 7/VI. Doubtless Dr. Erich Huettenhain of OKW/Chi who is reported as being one of the best of the German cryptanalysts in the mathematical field also took a look at it. Anyway Fritz Menzer also an expert in the development and testing of cipher machines with OKW/Chi is said to have tried to reconstruct this one vital part and to make the machine actually work, but without success. The Germans were quite definite in the opinion that from the point of view of cryptographic security the Russian K-37 was only conditionally sufficient. Of course the same may be said of almost any cryptographic system.

Assuming that cribs are available, it becomes merely a question of the loading or over-loading of the vehicle with traffic. With the one-time use of additive there is no question of overloading but a problem of sufficient production and distribution.

B. Transposition Systems

Double transpositions are said to have been employed in the radio traffic of Russian bands. The box widths were constant, that is for a given link, but the width of the A box was not necessarily the same as the width of the B box. The key words changed daily, but did recur from month to month. The Russian text was written in Latin letters by means of a transliteration. Punctuation marks were enciphered, for example, the period as TCK, the comma as SPT, etc. The address was always at the beginning and the signature at the end. If a message had several parts, "PROD SLED" or KONEC SLED" was placed at the end of the parts, PRODOLVENIE (PROD)" or "KONEC" at the beginning. Apparently there were no upper or lower limits to the message lengths. The numerical key for each box is derived from a key sentence. As many letters are counted off in the sentence as the tactical date of the message indicates. Beginning with the last of these letters a number of letters is taken which corresponds to the width of the box. If the sentence is not long enough, the series continues from the beginning. The key is determined in the usual fashion from the group of letters thus selected by numbering the letters according to their alphebetical sequence. When the same letter recurs, the one at the left receives the lower number. Both the keys thus obtained, one for the A box and one for the B box, are almost always read cyclically from a definite number on (1 to 7). In the enciphered message a blind or null group is inserted, its position being usually determined by the first number of the key, sporadically by the date (without using the tens, 0 equals 10th position). Encipherment is accomplished in the usual manner by writing the plain text horizontally in the rows of box A, taking the columns of this box in the numerical order as indicated by the key and writing the letters in the rows of the B box and finally taking the letters of these columns out in the order indicated by this numerical key to produce the cipher text.

C. Some Notes on Cryptographic Procedure

The following notes on cryptographic procedure are from the 1939 edition of "Regulations for Staff Cryptographic Service in the Red Army" (DF95):

(1) It is catagorically forbidden to encipher in the same code an order regarding the abolition of said code. If no other means are available the order must be transmitted through the cryptographic unit of the Peoples Commissariat for Internal Affairs.

(2) The sending of packages of cryptographic material is through the field connections of the NKVD and the pouches are inscribed: "Strictly Secret: Series "K". To the Chief of the Staff Cryptographic Unit of the troop unit .....personally".

(3) The recipient of cryptographic materials confirms to the sender on the day of receipt by an open telegram of Series "G" by military telegraph (if available): "Your number....with enclosure received in good order, (day and month)", or by a report via the field connection.

(4) The designations "Series G" and "Series K" seem to be priority ratings since in this document there is found also the references:

(a) Operational documents (battle orders and reports) are stamped with the imprint "cipher text of series "G" urgent". Cipher text of series "G" are worked on and delivered without delay.

(b) Cipher texts with collective data, e.g. of personnel, equipment, custody of material, etc., for a district or army are to be sent stamped, "cipher text, series "K"".

(c) Cipher texts (aside from series "G" and "K") addressed to the Central Committee of the Communist Party to the Council of the Peoples Commissars of the U.S.S.R., to the Peoples Commissar for the Defense of the U.S.S.R., or to the Chief of General Staff of the Red Army, of the War Council, and of the Staff of the Military District are stamped "Cipher text "G"".

(d) All other messages are stamped "cipher text".

(5) Encipherment of punctuation marks in cipher text is obligatory. However the period at the end of the cipher text is not enciphered.

(6) Address, date, month, year and words like troop unit, map coordinates and cover signature stand out from the general message text and constitute the "data". The "data" are enciphered in the midst of the message text. To set them off from the message text they are preceded by "data" and followed by "end of data".

(7) Proper names and especially important data (places, numbers, time, etc.) where garbling is especially dangerous, must be repeated in the encipherment.

(8) Especially long messages are to be broken up into separate parts (150-200 groups in each part), which are to be enciphered and sent independently. When breaking up a message into several parts the "data" are incorporated in the first part of the message. At the end of the first and ensuing parts is added enciphered "continuation follows", in the next to the last part "conclusion follows". Furthermore at the beginning of the following parts there is inserted enciphered "first continuation of Message number....", "second continuation of message number....", etc. and in the final part "end of message number....". Each part of such a message must have the appearance of a complete cipher text and must be registered under a separate, individual number.

(9) If parts of a message be garbled, then a request is made, enciphered, for the garbled passages (from such and such a word to such and such a word) e.g.: "Repeat No. -- from the word (group) "Our troops" to the word "the enemy is in possession of".

(10) The repetition of single groups or of the entire message is requested in clear, e.g. "Your message No. -- repeat the 5th and 6th groups".

In these regulations the activities of the Staff Cryptographic Units in time of war were outlined also with final stress being placed on the importance of captured enemy material.

Para 140. "The prompt utilization of cryptographic material of the enemy is of great importance for the success of our operations. Therefore, if our troops capture codes, means of encipherments, commander codes, traffic codes, cipher texts and other similar documents of the enemy, everything must be done to pass the captured material as quickly as possible to the intelligence agencies".

VI. THE AREAS AND DATES OF USE OF THE BASIC SYSTEMS

A. In the Red Worker and Peasant Army

(1) The 5-figure chiffre codes were used by the General Staff, Front Staff, Army, Corps, Division and Brigade.

(a) 011-A was in use from Jan. 41 to Oct. 41.

(b) 023-A was in use from Oct. 41 to March 42.

(c) 045-A was in use from March 42 to March 43.

(d) 062-A was in use from March 43 to March 44.

(e) 091-A was in use from March 44 to May 45.

(2) The 4-figure code books were used by Army, Corps, Division, Brigade and Regiment.

(a) OKK-5 was used from June 39 to June 40.

(b) OKK-6 was used from June 40 to Sept. 41.

(c) OKK-7 was used from Sept. 41 to Jan. 42.

(d) OKK-8 was used from Jan. 42 to March 42.

(e) OSKK-7 was used from Aug. 41 to March 42.

(3) Various 2, 3 and 4-figure systems known as SUV were used by Army, Corps, Division, Brigade, Regiment, Battalion and Company from 1942 to 1945.

(4) Various 2-figure systems known as PT were used by Regiment, Battalion, Company and Platoon from 1933 to 1942.

(5) Various 3-figure code books or tables were used by the Army Air Force. The VAK-38 was in force in 1938.

B. In the Peoples Commissariat for Internal Affairs

(1) A 5-figure code book was used by the GUP NKVD, Front Staff, Division, Unit, and Regiment from 1943 to 1945.

(2) Various 4-figure code books were used by the GUP NKVD, Front Staff, Division, Unit and Regiment from 1935 to 1945.

(a) ZERNO was used from 1943 to 1945.

(b) VIZA was used from 1943 to 1945.

(c) NIVA was used from Feb. 45 to May 45.

(3) Various 2,3 and 4-figure systems similar in structure to SUV were used by Division, Unit, Regiment, Batallion, Field Post, Operational Group and Guard Group from 1942 to 1945.

(4) Various 2-figure systems similar in structure to PT tables were used by Regiment, Batallion, Field Post, Operational Group and Guard Group from 1933 to 1942.

APPENDIX A

The listing by DF number and title of all the documents covered in the preparation of this paper.

DF. NO.	TITLE
68	Vneshtorg Encipherment Systems 1924-26.
74	On the Russian Cipher Machine K-37.
75	Breaker's Aid for Word Codes.
76	Studies of Russian Double Transposition.
78	Russian Cipher Systems - Kurt Friederichsohn.
81	Cipher Systems of Russian Agents and Partisans.
85	Survey of Latest Status of Decipherment of Soviet Systems.
86	Solution of R4ZC1500 NKVD Western Front.
87	Solution of R4ZC 3000.
89	Details of Russian Cryptologic Organization - Learned from German Interrogation of Russian Prisoners of War.
90	Russian Word Pattern Book.
93	Three Russian Agent Systems.
94	The Development of Russian Cryptographic Systems.
95	Regulations for Staff Cryptographic Service in the Red Army.
97	Encipherment of OKK-6.
98	Forschungsamt Solution of Russian Teletype Scrambler.
111	Comments on Various Cryptologic Matters - Adolf Paschke.
112	Survey of Russian Military Systems - Alex Dettmann.
115	Explanation of a Small Russian Code.
116-L	Activity of the German Radio Defense Corps - Wilhelm Flicke.
116-AH	Radiograms of the Rote Drei - Wilhelm Flicke.
122	Russian Linguistic Peculiarities Assisting Cryptanalysis - Alex Dettmann.
125	Russian Airforce Law Echelon Proforma Messages.
126	Examples of (Russian) Substitution Tables.
133	Results of Textual Studies of Russian Military and Political Cryptograms.

DF. NO.	TITLE
135	Russian Radio Agents in 1942.
136	Methods of Cryptanalysis - Dettmann.
138	Methods of Decipherment - Dettmann.
139	Methods of Decipherment - Dettmann.
140	Two Russian PW Interrogations.
141	Methods of Decipherment - Dettmann.
143	Manual for the Analysis and Utilization of Radio Intelligence Material.
144	Methods of Decipherment - Dettmann.
145	Methods of Decipherment - Dettmann.
146	Methods of Decipherment - Dettmann.
152	Cryptanalytic Report (For the Fourth Quarter 1944).
154	Methods of Decipherment - Dettmann.
155	Methods of Decipherment - Dettmann.
156	Methods of Decipherment - Dettmann.
157	The General Trend of the Russian Codes - Lt. Col. Yamada (Japanese).
158	General Outline of the Codes used by the Red Army Ground Forces, Air Forces, and Border Guard Units - Fukunaga Eiichi (Japanese).
162	Interrogation of Japanese National, Kawarabayashi, Tashikazo.
163	Interrogation of Japanese National, Otani, Fukashi.
164	Interrogation of Japanese National Kawaoka, Tadao.
165	Methods of Decipherment - Dettmann.
166	Methods of Decipherment - Dettmann.
167	Methods of Decipherment - Dettmann.
168	Methods of Decipherment - Dettmann.
171	Methods of Decipherment - Dettmann.
175	Methods of Decipherment - Dettmann.
179	Methods of Decipherment - Dettmann.
180	Methods of Decipherment - Dettmann.

TOP SECRET SUEDE

NEVER TO BE SEEN BY UNAUTHORIZED PERSONS.

DF. NO.	TITLE
182	Report by Waldemar Penner formerly attached to Signal Intelligence Service, German Air Force.
183	Decipherment as a Source of Intelligence.
184	Interrogation of Japanese National Kishimoto, Koishi.
187-B	The Cryptanalytic Successes of OKW/Chi after 1938. - Wilhelm Fenner.
196	Report on Russian Decryption in the Former German Army. - Alex Dettmann and Sergius Samsonow.
206	Cryptanalytic Aid for Word Codes.
216	Radio Traffic and Methods of Encrypting in the Soviet Air Force up to May 1945.
217	The Russian Cipher Device K-37.
5/49/TOPSEC/AS-14-TICOM	The Russian Communications Security Organization During World War II.